スマートフォンを利用している方へ

最近、スマートフォンを利用する人が増えています。

便利なスマートフォンですが、携帯電話と同じ感覚で使用していると、思わぬトラブルに巻き込まれる可能性もあります。

スマートフォンは携帯電話とは異なり、パソコンに電話機能が付いたものと考えてください。このため、パソコンと同様のセキュリティ対策が必要です。
スマートフォンを標的としたウイルスも発見されており、被害にあわないためにも、スマートフォンが抱えている問題点をしっかりと把握し、適切な対策を行うことが大切です。

【保護者の方へ】
お子さんがスマートフォンを使用する場合は、本当に必要なのか、その必要性をよく考えてください。
また、利用する際には必ずフィルタリングを設定しましょう。スマートフォンの場合は携帯電話と異なり、Wi-Fi（無線ＬＡＮ）経由のアクセスでもフィルタリングが動作するよう、保護者自身が適切な設定を行う必要があります。

※フィルタリングの設定については、各携帯電話会社等へお問い合わせください。

相談事例

・スマートフォンでインターネットをしていたら、不当料金請求の画面になってしまい、高額な利用料金を請求された。

こちらをご覧ください：ワンクリック料金請求にご用心

・スマートフォンが、自分の個人情報や位置情報を勝手にどこかへ送信しているようで心配だ。

被害防止策

「おかしいな」と思ったら、スマートフォンの通信設定や、導入しているアプリケーション（アプリ）の設定をもう一度よく見直してみましょう。外部へのデータ送信を許可しているアプリがあるかもしれません。

特に、自由にアプリを配布・インストールすることができるAndroid端末を利用している方は、端末内の情報を勝手に外部へ送信するなどの不正なアプリに十分注意してください。

アプリをインストールする前に、レビューを見たり、インターネットで検索してみるなど、事前に情報収集することで、被害を未然に防ぐこともできます。

【共通事項】

・ウイルス対策ソフト（ウイルス対策アプリ）を導入し、常に最新のパターンファイルに更新しておく
・システムやアプリは常にアップデートし、最新の状態を保つ
・端末自体に設けられた制限を取り外すなど、スマートフォンを改造しない
・外部に漏れると困るようなデータは保存しない
・暗証番号を設定し、もし紛失してしまったとしても、他人が勝手に操作できないようにする

【Android端末の場合】

・アプリをダウンロードする際には信用できるサイトから行い、作成者や提供元が不明のアプリはダウンロードしない
・アプリをインストールする際は、「アクセス許可」を必ず確認し、アプリの動作から考えると不必要なアクセス権限を求められていないか、よく確認する

アクセス許可に注意しよう（Android端末を利用している方）

アプリの「アクセス許可」とは、アプリがAndroidの、どの情報・機能にアクセスをするのか定義したものです。
個人情報等を端末から不正に盗み取り、外部に送信するような不正アプリは、アプリの種類や動作から考えると、不自然なアクセス許可をユーザに求めてくることがあります。アプリをインストールする際には、アクセス許可を必ず確認しましょう。

【アクセス許可の例（一部）】
※お使いの機種やアクセス状況によって、表示（表現）が異なる場合があります。

アプリによっては、アクセス許可の一覧の一部しか表示されないこともあります。その場合は「すべて表示」ボタンを押して確認をしてください。

アクセス許可	説明
電話発信	アプリが電話番号や端末識別番号、SIM情報を読み取ることができます。
個人情報	アプリがアドレス帳などのデータを読み取ることができます。
位置情報	アプリがスマートフォンの位置情報を知ることができます。
ネットワーク通信	アプリがインターネットを利用し、情報を送受信することができます。
SMSメッセージの送信	SMSメッセージの送信をアプリに許可します。悪意のあるアプリが知らない間に メッセージを送信し、料金が発生することがあります。

アプリが「電話発信」、「個人情報」、「位置情報」と「ネットワーク通信」のアクセス許可を求めてきた場合、電話番号や電話帳、位置情報といった情報が、インターネットを通じて第三者に送信されてしまう可能性があります。

例えば、強力な光を放つ機能のみの「懐中電灯アプリ」があったとします。

このアプリのアクセス許可に「ネットワーク通信」と「個人情報」「電話発信」「位置情報」は必要ないはずです。

アクセス許可の表示画面例

この場合、自分の電話番号やメールアドレス、電話帳のデータ、位置情報がインターネットを通じて第三者へ送信される可能性があります。

◆正当な目的に使用されるアクセス許可なのか分からない場合

アクセス許可が、正当な目的に利用されるのか分からない場合は、一旦インストールを中止してください。その後、

・アプリのレビュー欄を読み、他のユーザの評判を見てみる
・開発者や開発元が信頼できるか確認する
・インターネットでアプリについて検索をかけてみる
・正規のアプリとよく似た、偽アプリが報告されていないか確認する

などアプリについての情報収集を行い、総合的に判断をするようにしてください。

◆無料アプリに要注意

「無料」アプリは、なぜ無料なのか、考えてみたことはありますか？
あなたの端末内に保存されている個人情報と引き換えに「無料」なのかもしれません。

また、正規のアプリケーション配布サイトに掲載されているアプリであっても、監視や審査を逃れて不正なアプリが紛れ込んでいる可能性はゼロではありません。

アプリをインストールする際には、「アクセス許可」を確認し、本当に必要な権限なのか判断してからインストールしましょう。

GPS機能にも注意

スマートフォンで写真を撮影すると、端末のＧＰＳ機能により、撮影した写真に緯度経度情報が含まれる場合があります。
このため、不用意に自宅で撮影した写真をインターネット上に公開すると、緯度経度情報から自宅が特定されてしまうこともあります。

スマートフォンのＧＰＳ機能の設定がどうなっているのか、よく確認してください。

東京くらしＷＥＢ くらしに関わる東京都の情報サイト
スマートフォン等で撮影した写真をブログにアップすると撮影場所が特定されることがあるので注意しましょう

参考ページ

情報セキュリティ上の様々な脅威への対策を分かりやすく解説した「IPA対策のしおりシリーズ」のページもご覧ください。

○ ＩＰＡ 独立行政法人 情報処理推進機構

IPＡ 対策のしおりシリーズ８
スマートフォンのセキュリティ＜危険回避＞対策のしおり
http://www.ipa.go.jp/security/antivirus/shiori.html

「スマートフォンを安全に使おう！」
http://www.ipa.go.jp/security/txt/2011/08outline.html

「あなたを狙うスマホアプリに要注意！」
～不正なアプリをインストールしてしまわないために～
http://www.ipa.go.jp/security/txt/2012/05outline.html

Android OSを標的とした不審なアプリに関する注意喚起
http://www.ipa.go.jp/security/topics/alert20120523.html

警視庁サイバー犯罪対策課では、サイバー犯罪に係る相談や情報提供を電話で受け付けています。

ミヨミライハイテク

電話相談　03-3431-8109

受付時間は、平日の午前8時30分から午後5時15分までです。
夜間及び祝日・土日は、相談業務を行っていません。

ワンクリック料金請求にご用心

クリックしただけで料金請求？

　最近、パソコンや携帯電話、スマートフォンを使いインターネットに接続し、サイトを閲覧していたら、年齢認証を求められクリックしたところ、一方的に会員登録となり、高額な料金を請求されるという相談が多く寄せられています。

不当な請求に応じないよう、次のことを参考にしてください。

慌てて支払わない

　クリックしただけで、直ちに契約は成立しないので、まずは最寄りの消費生活センターで相談をしてください。利用規約があったとしても、契約が成立していない場合が多いので、慌てず、落ち着いて対応してください。

個人情報は分からない

　パソコンのＩＰアドレスや、携帯電話の個体識別番号から個人情報は分かりませんので、これらの情報が画面に表示されたとしても慌てないでください。
自分から相手に教えない限り、個人情報は分かりません。

【スマートフォンの場合に注意！】

※ Android OSのスマートフォンにおいて、料金請求画面に自分の電話番号やメールアドレスが表示された場合は、不正なアプリケーション（アプリ）によって、端末の個人情報等が相手業者に伝わっている可能性があります。
相手業者から料金請求の電話がかかってきたり、メールが送られてきた場合は、電話の着信拒否やメールの受信拒否等で対応してください。

Android端末の場合は、アプリのインストール時にアクセス許可をよく確認することが大切です。アプリの動作から考えると、不必要なアクセス許可があるものは、インストールを中止してください。
また、提供元が不明など、信頼できないアプリはインストールしない設定にしてください。

※参考にしてください
ＩＰＡ 独立行政法人 情報処理推進機構
コンピュータウイルス・不正アクセスの届出状況[１月分]について
「スマートフォンでもワンクリック請求に注意！」

※スマートフォンのセキュリティ対策についてはこちらを参考にしてください

ＩＰＡ 独立行政法人 情報処理推進機構 対策のしおりシリーズ８
スマートフォンのセキュリティ<危険回避>対策のしおり（第１版）

相手業者に連絡をしない

相手業者に電話をしたり、確認のメールを送ったりすることは、相手に自分の連絡先を伝えてしまうことになるので注意してください。

相手業者に連絡すると、代金の支払いに関してメールが大量に届いたり、電話がかかってくる場合があります。メールがたくさん届くようになった場合は、メールの受信拒否をする方法などがあります。また、電話がかかってくる場合は着信拒否の設定をしましょう。詳しくは、各携帯電話会社に問い合わせてください。

※参考にしてください

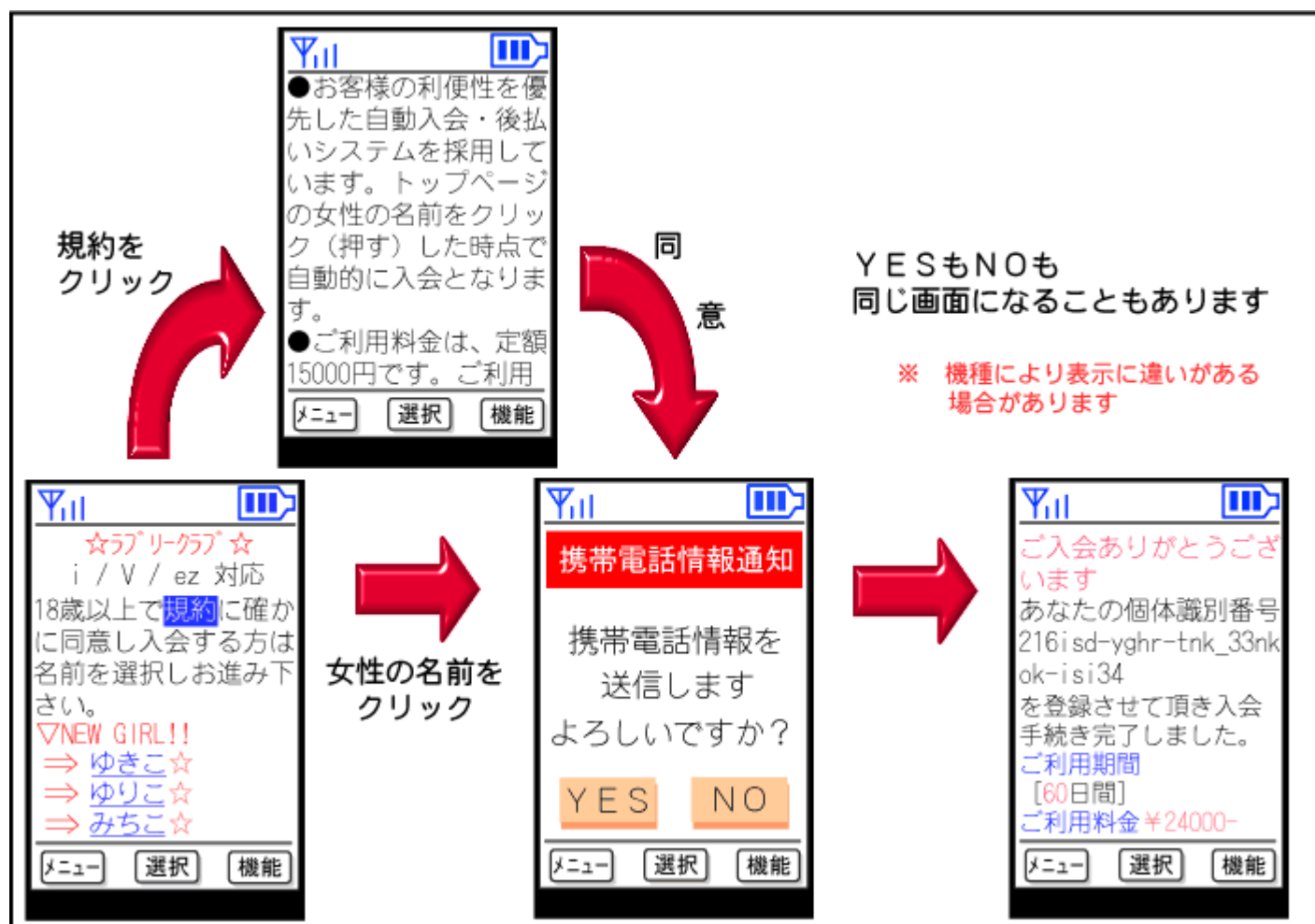
不正な登録・料金請求画面は消せる

　動画だと思ってダウンロードしたものが、料金請求画面を表示する不正なプログラムであり、パソコンのデスクトップ上から消えないことがあります。このような場合は、「システムの復元」という機能を使えば消える場合があるので、情報処理推進機構の解説を参考にして対応してください。

※システムの復元の実施に当たっては、説明をよく読み、自己責任でお願いします。

○こちらのページもご覧ください
料金請求画面が消えない

ワンクリック料金請求サイトの表示例

　認証画面をクリックして次に進んだところ、料金の説明や、入会登録するにあたり、契約の確認画面が一切なかったにも関わらず、急に「登録完了」と表示されるようです。
同様に、パソコンに送られてきたメールに記載されているＵＲＬをクリックしただけで、料金請求画面が表示される場合もあります。
相手の連絡先が記載してあったとしても、自ら連絡せず、無視することが一番よい対処法です。

YESはもとより、NOをクリックしても

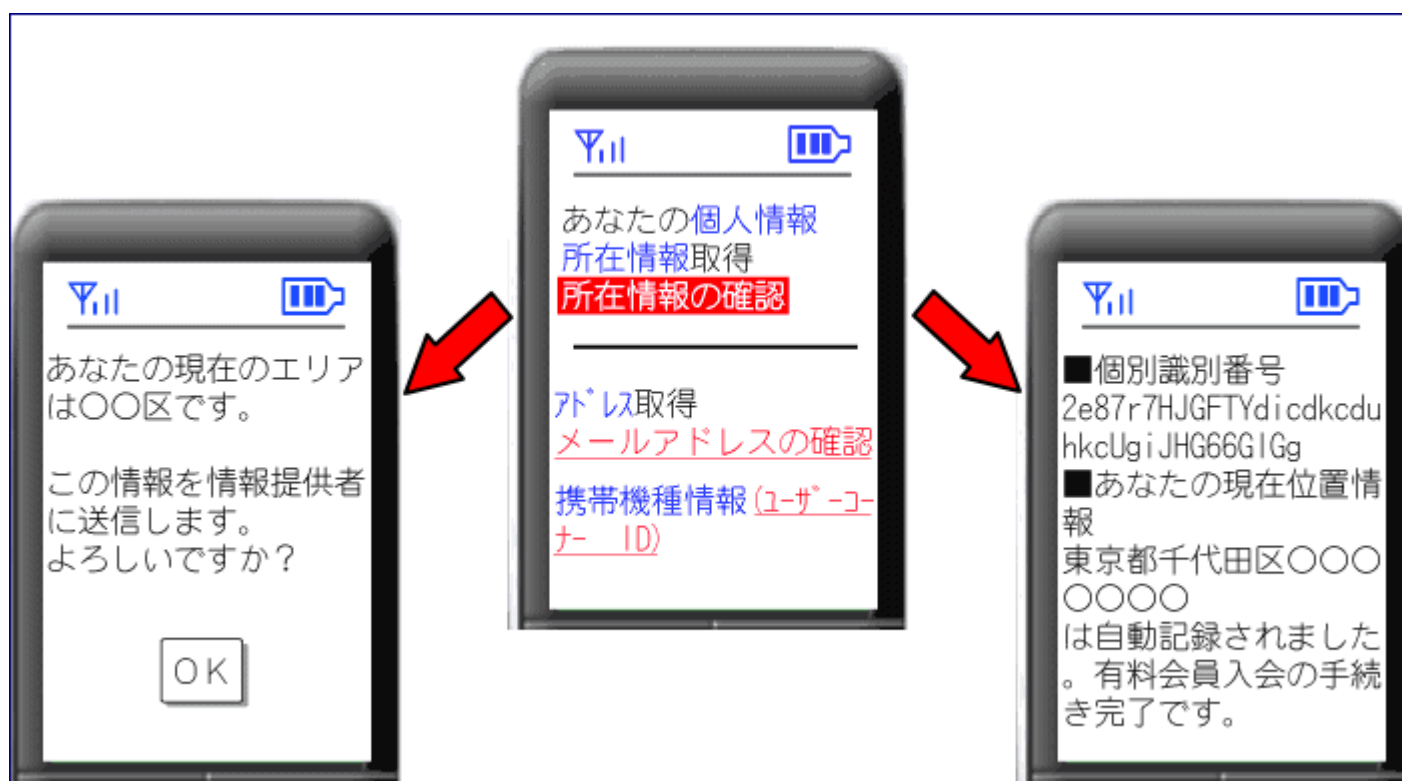
YESをクリックしたのと同じ画面に進んでしまうことも・・・

多くの不当料金請求のサイトには、金額だけではなく、
「ご登録完了しました。」
「携帯電話情報を送信します。」
「あなたの個体識別番号はxxxxxです。手続きを完了しました。」

・・・などと記載されています。

実際に自らサイトにアクセスしたことによって料金請求の画面が表示されるため、驚いてしまう人が多いようです。

たとえ携帯電話の機種名や個体識別番号、自分の位置情報が事実だったとしても、それらの情報から個人情報が漏れてしまうことはありません。もっともらしく文面に記載されていることをすぐに信じたりせず、料金の支払いや返信をしないようにしましょう。

位置情報が記載されたワンクリック料金請求画面のイメージ例

たとえ、このような画面が表示されても
位置情報から個人情報がもれることはありません！

　これらの不当な料金請求は、出会い系サイトやアダルトサイトによく見られます。怪しいサイトには、最初からアクセスをしないようにお願いします。
また、一方的に送られてくる勧誘メールに安易に登録したり、おもしろ半分や興味本位で、届いた勧誘・広告メールに記載されたURLをクリックするのはやめましょう。

特に、お子さんが不当料金請求にあってしまった場合は、どうしてそのようなサイトにアクセスできてしまったのか、フィルタリングの設定をよく見直してください。

料金請求の手段があまりにも悪質である場合、又は支払いに応じてしまった場合などは、最寄りの警察署へご相談ください。

参考ページ

架空請求の情報を集めています。（東京都 架空請求緊急対策班）

利用した覚えのない「料金請求」注意！（警視庁）

個人情報を入手していると偽って請求行為を行うサイトについて(NTTドコモ)

警視庁サイバー犯罪対策課では、サイバー犯罪に係る相談や情報提供を電話で受け付けています。

ミヨミライハイテク

電話相談　03-3431-8109

受付時間は、平日の午前8時30分から午後5時15分までです。
夜間及び祝日・土日は、相談業務を行っていません。

▲このページのトップへ

くらしに関わる東京都の情報サイト

検索 文字サイズ：小さく 標準 大きく

サイトマップ 背景色を変更：標準 白 黒 青

東京くらしWEB ホーム ＞ 相談したい ＞ ご注意ください（消費者被害情報ほか） ＞ スマートフォン等で撮影した写真をブログにアップすると撮影場所が特定されることがあるので注意しましょう。

スマートフォン等で撮影した写真をブログにアップすると撮影場所が特定されることがあるので注意しましょう。

消費生活アドバイス

平成23年12月2日

スマートフォン・携帯電話のカメラやデジタルカメラには、GPSと連動させる機能のある機種があり、旅先で撮った写真等の位置情報を残すことができます。しかし、位置情報の付加設定をONにしたまま撮影し、その写真をブログ（インターネット上の日記）にアップすると、意図せずに位置情報をインターネット上に公開してしまうこともありますので、注意が必要です。

相談事例

スマートフォンで撮った室内の写真をブログにアップしたところ、位置情報を第三者に知られてしまった。

数年来、ブログを更新しており、お気に入りの写真をデジカメで撮ってブログに載せている。最近スマートフォンを購入し、スマートフォンで撮った写真をアップしたところ、知人から「写真をクリックすると自宅住所がわかってしまう」と注意された。写真のデータ情報を見ると、緯度経度が載っておりネット上の地図で確認すると、所在地がわかってしまう。携帯電話会社へ問い合わせたところ、設定により非表示にすることができると言われたが、知らない人も多いと思う。

（50代 女性）

～アドバイス～

写真をインターネット上で公開する際は、自分のスマートフォン、デジカメ等にGPS機能がついているか確認し、不要であれば、GPS連動の設定はOFFにしましょう。

スマートフォン、携帯電話、GPSを内蔵したデジカメ等には、撮影時にジオタグ(写真画像やデジタルデータに添付する位置情報)を画像に付加する機能がついている商品があります。旅行先などで撮った写真の撮影場所がわかる機能はとても便利ですが、使い方を誤ると、自分の個人情報を期せずして第三者へ開示することになります。

購入時に既に位置情報の付加設定がONになっている機種もありますので、自分が使用して

計量検定所

いる機器を確認し、不要であれば設定をOFFにしましょう。

以上、スマートフォンやデジカメなどの位置情報に起因する特徴をよく理解したうえで、賢く利用しましょう。

関連情報

[2011年9月16日]
【アドバイス】スマートフォンは思わぬ不具合が起こる可能性もあります。

[2011年8月8日]
【アドバイス】スマートフォンは特徴を理解したうえで賢く利用しましょう！

◎ スマートフォン等の契約についておかしいなと思ったら、すぐに最寄りの消費生活センターにご相談ください。

お問い合わせ先

東京都消費生活総合センター 電話03－3235－1155（相談専用電話）

東京くらしWEBトップへ　このページのトップへ

東京都生活文化局消費生活部　東京都消費生活総合センター　東京都計量検定所

情報セキュリティ

ENGLISH

- 読者層別
  - 個人の方
  - 経営者の方
  - システム管理者の方
  - 技術者・研究者の方
- 緊急対策情報
- 届出・相談
  - ウイルスの届出
  - 不正アクセスの届出
  - 脆弱性関連情報の届出
- 情報セキュリティ対策
  - 制御システム
  - ウイルス対策
  - ボット対策
  - 不正アクセス対策
  - 脆弱性対策
  - 対策実践情報
- 暗号技術
- セキュリティエコノミクス
- 情報セキュリティ認証関連
  - JISEC
  - JCMVP
- セミナー・イベント
- 資料・報告書・出版物
- ツール
- 公募
- サポート情報
  - 用語集
  - FAQ（よくある質問）
  - セキュリティ関連リンク
- セキュリティセンターについて

IPA対策のしおりシリーズ

- 情報セキュリティ上の様々な脅威への対策を分かりやすく解説 -

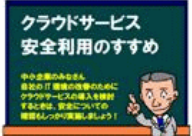
最終更新日 2012年10月18日
独立行政法人情報処理推進機構
技術本部 セキュリティセンター

「IPA対策のしおりシリーズ」は、一般のご家庭や企業（組織）内でパソコンやスマートフォンをご利用する方々を対象に、情報セキュリティ上の様々な脅威への対策を分かりやすく説明した小冊子です。これらの脅威への対策を実践するために、ぜひご活用ください。

なお、営利を目的としない用途に限り、原本のまま印刷し、配布することに関して、制限はございません。

IPA対策のしおりシリーズ

1	ウイルス対策のしおり	ウイルス対策のしおり(第9版)（839KB） ～ コンピュータウイルスからあなたのパソコンを守るには!!～	[英語版] (1.6MB)
2	スパイウェア対策のしおり	スパイウェア対策のしおり(第10版)（822KB） ～気付かぬうちにスパイウェアに侵入されていませんか？～	[英語版] (4.4MB)
3	ボット対策のしおり	ボット対策のしおり(第9版)（1.0MB） ～あなたのパソコンはボットに感染していませんか？～	[英語版] (2.1MB)
4	不正アクセス対策のしおり	不正アクセス対策のしおり(第6版)（779KB） ～大丈夫ですか、あなたのパソコン？（パソコン利用者向け）～	[英語版] (3.2MB)
5	情報漏えい対策のしおり	情報漏えい対策のしおり(第6版)（795KB） ～企業(組織)で働くあなたへ7つのポイント !!～	[英語版] (6.8MB)
6	インターネット利用時の危険対策のしおり	インターネット利用時の危険対策のしおり(第4版)（1.6MB） ～インターネットに潜む悪意 こんな手口に騙されないで!!～	[英語版] (1.8MB)
7		電子メール利用時の危険対策のしおり(第4版)（1.1MB） ～電子メールを介したトラブル こんな対策が必要で	[英語版] (1.0MB)

		す!!～	
8		[スマートフォンのセキュリティ<危険回避>対策のしおり(第2版)] （1.2MB） ～便利な道具 スマートフォン 安全・安心利用のためのセキュリティ対策で危険回避!!～	[[英語版]] (1.0MB)
9		[初めての情報セキュリティ対策のしおり(第1版)] （1.3MB） ～新入社員の皆さん「情報セキュリティ対策」って知っていますか？～	[[英語版]] (1.2MB)
10		[標的型攻撃メール<危険回避>対策のしおり(第1版)] （1.２MB） ～特定企業･組織への狙い撃ち攻撃 その発端となる最初の攻撃はメールから始まる!!～	[[英語版]] (0.8MB)

IPA対策のしおりシリーズの一部の冊子については英語版を公開しています。
IPA対策のしおりシリーズの英語サイトはこちらにあります。

IPAセキュリティマネジメントのしおりシリーズ

本シリーズは、情報セキュリティ対策を実施する企業・組織の経営者、管理者、従業者の方々を対象とした小冊子です。

1		企業(組織)における最低限の情報セキュリティ対策のしおり （4.5MB） New
2		中小企業における組織的な情報セキュリティ対策ガイドライン チェック項目 （0.9MB） New
3		中小企業における組織的な情報セキュリティ対策ガイドライン 事例集 （0.8MB） New
4		情報セキュリティ対策ベンチマーク (企業・組織のためのセキュリティ対策自己診断ツール Ver.4.x) （1.6MB） New

姉妹冊子

	クラウドサービス安全利用のすすめ （2.5MB） ～中小企業のみなさん 自社のIT環境の改善のためにクラウドサービスの導入を検討するときは、安全についての確認もしっかり実施しましょう！～	[英語版] (2.7MB)
	情報漏えい発生時の対応ポイント集 （0.8MB） ～情報が漏えいしてしまった時、何をすべきか!! ～	

関連資料

- ボット対策について
- パソコンユーザのためのスパイウェア対策 5 箇条
- 15分でわかるウイルスの脅威
- ウイルス対策スクール

お問い合わせ先

IPA 技術本部 セキュリティセンター
Tel: 03-5978-7508 Fax: 03-5978-7518 E-mail: isec-info@ipa.go.jp

変更履歴

- 2012年10月18日 「IPAセキュリティマネジメントのしおりシリーズ」(1)～(4)を公開
  「情報漏えい発生時の対応ポイント集」を公開
- 2012年10月1日 「電子メール利用時の危険対策のしおり」英語版を公開
- 2012年9月25日 「インターネット利用時の危険対策のしおり」英語版を公開
- 2012年9月5日 「中小企業における最低限の情報セキュリティ対策のしおり」を公開
- 2012年9月3日 「スマートフォンのセキュリティ対策のしおり」英語版を公開
  「標的型攻撃メール対策のしおり」英語版を公開
- 2012年6月21日 「ウイルス対策のしおり」を改版(第9版)
  「スパイウェア対策のしおり」を改版(第10版)
  「ボット対策のしおり」を改版(第9版)
  「不正アクセス対策のしおり」を改版(第6版)
  「情報漏えい対策のしおり」を改版(第6版)
  「インターネット利用時の危険対策のしおり」を改版(第4版)
  「電子メール利用時の危険対策のしおり」を改版(第4版)
  「スマートフォンのセキュリティ対策のしおり」を改版(第2版)
  「初めての情報セキュリティ対策のしおり」英語版を公開
  その他、IPA対策のしおりシリーズの英語版のリンクを追加
- 2012年1月30日 「初めての情報セキュリティ対策のしおり」を公開
  「標的型攻撃メール対策のしおり」を公開
  「クラウドサービス安全利用のすすめ」(日本語版・英語版)を公開
- 2011年10月25日 「スマートフォンのセキュリティ対策のしおり」を公開(第1版)
  「ウイルス対策のしおり」を改版(第8版)
  「スパイウェア対策のしおり」を改版(第9版)
  「ボット対策のしおり」を改版(第8版)
  「不正アクセス対策のしおり」を改版(第5版)
  「情報漏えい対策のしおり」を改版(第5版)
  「インターネット利用時の危険対策のしおり」を改版(第3版)
  「電子メール利用時の危険対策のしおり」を改版(第3版)
- 2009年12月14日 掲載

ページトップへ

独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

Googleカスタム検索 検索

IPAについて サイトマップ お問合せ ENGLISH

HOME 情報セキュリティ ソフトウェア・エンジニアリング IT人材育成 情報処理技術者試験 未踏 国際標準の推進

HOME >> 情報セキュリティ >> ウイルス対策 >> ウイルスの発見届出状況 >> 記事

情報セキュリティ

ENGLISH

読者層別
- 個人の方
- 経営者の方
- システム管理者の方
- 技術者・研究者の方

緊急対策情報
届出・相談
- ウイルスの届出
- 不正アクセスの届出
- 脆弱性関連情報の届出

情報セキュリティ対策
- 制御システム
- ウイルス対策
- ボット対策
- 不正アクセス対策
- 脆弱性対策
- 対策実践情報

暗号技術
セキュリティエコノミクス
情報セキュリティ認証関連
- JISEC
- JCMVP

セミナー・イベント
資料・報告書・出版物
ツール
公募
サポート情報
- 用語集
- FAQ（よくある質問）
- セキュリティ関連リンク

セキュリティセンターについて

コンピュータウイルス・不正アクセスの届出状況[7月分]について

第11-28-226号
掲載日：2011年 8月 3日
独立行政法人情報処理推進機構
技術本部 セキュリティセンター(IPA/ISEC)

IPA（独立行政法人情報処理推進機構、理事長：藤江 一正)は、2011年7月のコンピュータウイルス・不正アクセスの届出状況をまとめました。
(届出状況の詳細PDF資料はこちら)

1. 今月の呼びかけ

「 スマートフォンを安全に使おう！ 」

IPAでは2011年2月にスマートフォンのウイルスに関する呼びかけ※1を発表しましたが、その後も新しいウイルスが次々と発見されており、利用者にとってウイルス感染の脅威はますます高まってきています。
また、ここ最近のIPAのウイルス届出の状況においても、スマートフォン（特にAndroid端末）を狙ったウイルスが検出され始めています。
このような状況を考慮し、今回改めてスマートフォンをとりまくウイルス事情を解説するとともに、スマートフォンを安全に使うためにとるべき具体的な手段を紹介します。

※1 IPA-2011年2月の呼びかけ「スマートフォンのウイルスに注意！」
http://www.ipa.go.jp/security/txt/2011/02outline.html

図1-1：スマートフォンがウイルスに狙われつつあるイメージ図

(1)最近のスマートフォンのウイルス事情

表1-1はこれまでIPAに届出のあった、Android端末を狙ったウイルスの一覧です。

表1-1：IPAに届出のあった、Android端末を狙ったウイルス

届出時期	名称	特徴
2011年3月	AndroidOS/Lotoor (ロトール) [DroidDream] （ドロイドドリーム）	ウェブサイトからダウンロードすることにより感染し、Android 端末に保存されている情報を収集、外部に送信するといった機能を有する。
2011年6月	AndroidOS/Lightdd ライトディーディー	感染すると、Android端末の情報を盗み取り、外部に送信する。
2011年6月	AndroidOS/Smspacem エスエムエスパーセム	感染すると、Android端末内のアドレス帳の連絡先に、SMS※2メッセージの送信を試みる。
2011年6月	AndroidOS/Smstibook エスエムエスティブック	感染すると、事前に設定された番号に、プレミアムSMS※3メッセージの送信を試みる。

※2 SMS（Short Message Service）：携帯電話同士で、短い文章のメールを送受信できるサービス。
※3 プレミアムSMS：発信者がメッセージを送るだけで、相手先が利益を得る仕組みが付加されたSMS。

このように、今年に入ってからスマートフォンを狙ったウイルスが次々と発見されており、利用者にとってウイルス感染の脅威がますます高まってきています。
また、スマートフォンがウイルスに感染してしまった場合に想定される被害例として、以下が考えられます。

- スマートフォン内データ、GPS※4による位置情報等、個人情報を含む重要な情報が悪意ある第三者に送られてしまう。
- 悪意ある第三者にスマートフォンを乗っ取られて、自由自在に操られてしまう。
- スマートフォンがボットネット※5の1つとして組み込まれ、知らぬ間に特定の組織にサイバー攻撃を行うなどの犯罪の道具として使われてしまう。

※4 GPS（Global Positioning System）：人工衛星の電波を使って、受信者の地球上の位置を割り出すシステムのこと。
※5 ボットネット：攻撃者が、ボットと呼ばれるウイルスに感染させた多くのコンピュータを使って、ターゲットに対し遠隔で攻撃を行うために構築されたネットワークのこと。

(2)IPAに届出のあったスマートフォンのウイルスについて
図1-2は2011年3月～2011年7月に、IPAに届出のあったスマートフォンのウイルスの検出数のグラフです。

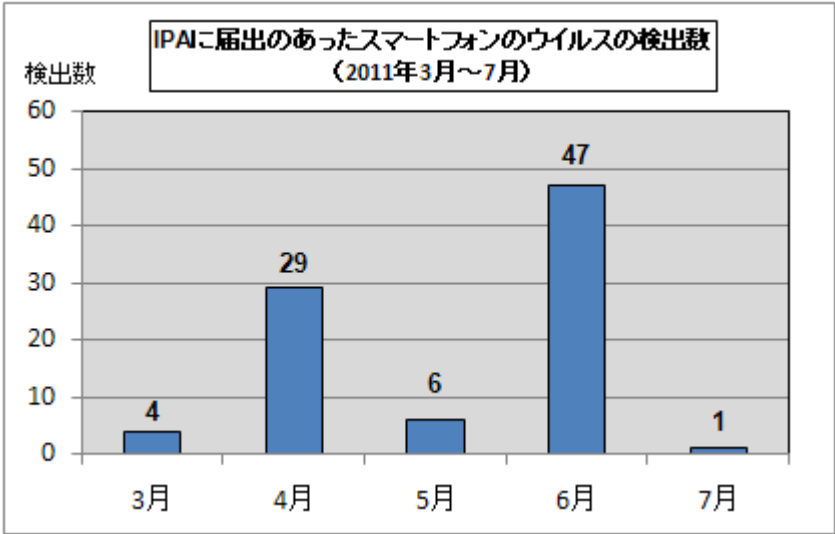



図1-2：IPAに届けられたスマートフォンのウイルスの検出数（2011年3月～7月）

これらのウイルスは全て、スマートフォン上で発見されたものではなく、Windowsなどパソコンの環境でメール受信時などに検出されたものでした。メールにウイルスを添付して、それをスマートフォン上で開かせることでウイルス感染させようという意図から、メールが不特定多数に送られたため、パソコンにも届いているようです。加えて、Android端末用のセキュリティソフトがあまり普及していないために、スマートフォン上でのウイルス発見の報告がまだないものと思われます。なお、2011年3月から7月に届出のあったスマートフォンのウイルスは、全てAndroid端末をターゲットとするものでした。
ウイルスが混入したアプリが添付されたメールをスマートフォンで受信した場合、スマートフォンの機種やOSによっても挙動が異なりますが、特に**Android端末の場合は**メール表示中の「インストール」ボタンを押すとアプリのインストールが開始され、ウイルスに感染してしまう場合があるため、取り扱いには十分注意する必要があります。
図1-3は、Androidアプリ（.apkファイル）が添付されたメールをスマートフォン（端末名：GALAXY Tab/OSバージョン：Android 2.2）上で見た際の画面例です。

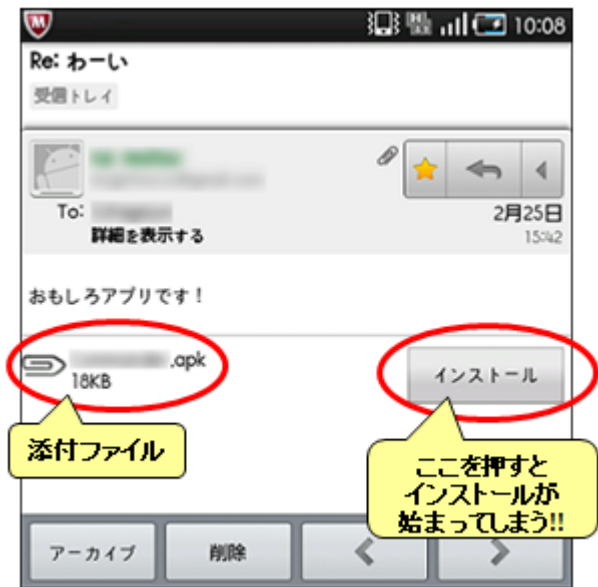



図1-3：Androidアプリが添付されたメールをスマートフォン上で見た画面例

(3)スマートフォンを安全に使用するための六箇条

上述したようなスマートフォンに関するウイルスの現状を受け、IPAでは特にウイルスと脆弱（ぜいじゃく）性を悪用した攻撃への対策を考慮した、スマートフォンを安全に使用するための六箇条をまとめましたので、スマートフォン使用時の指針としてください（図1-4参照）。

1. スマートフォンをアップデートする。
2. スマートフォンにおける改造行為を行わない。
3. 信頼できる場所からアプリケーション（アプリ）をインストールする。
4. アンドロイド端末では、アプリをインストールする前に、アクセス許可を確認する。
5. セキュリティソフトを導入する。
6. スマートフォンを小さなパソコンと考え、パソコンと同様に管理する。

図1-4：スマートフォンを安全に使用するための六箇条

各項目について以下に詳しく説明します。

【1】スマートフォンをアップデートする。

販売元からOSのアップデートが提供された場合、早めにアップデートしましょう。アップデートをしないで使っていると、パソコン同様、脆弱性を悪用した攻撃に遭う危険性が高まります。またその際、アップデート手順をきちんと理解することが重要です。アップデート手順は、販売元や製造元によって異なる場合があります。きちんとアップデートするために、取扱説明書などを確認し、正しい手順を身につけたうえでアップデートを実践しましょう。

【2】スマートフォンにおける改造行為を行わない。

スマートフォンにおける改造行為はやめましょう。ここでの改造行為とは、いわゆるiPhoneにおけるJailbreak（脱獄）やAndroid端末におけるroot権限奪取行為（root化とも呼ばれる）などのことを指します。スマートフォンで動作するウイルスの中には、改造行為を行ったスマートフォンのみに感染するものも確認されています。ウイルス感染の危険性を自ら高めてしまうことになりますので、スマートフォンの改造行為はやめましょう。

【3】信頼できる場所からアプリケーション（アプリ）をインストールする。

スマートフォンで使用するアプリは、iPhoneであれば米Apple社の「App Store」、Android端末であればアプリの審査や不正アプリの排除を実施している場所（米Google社の「Android Market」）など信頼できる場所からインストールしましょう。

【4】**Android**端末では、アプリをインストールする前に、アクセス許可を確認する。

Android端末の場合、アプリをインストールする際に表示される「アクセス許可」

（アプリがAndroid端末のどの情報／機能にアクセスするか定義したもの）の一覧には必ず目を通しましょう（図1-5参照）。過去発見されたAndroid端末を狙ったウイルスには、個人情報などを不正に盗み取るため、アプリの種類から考えると不自然なアクセス許可をユーザーに求めるものがありました。例としては、壁紙アプリにも関わらず、アドレス帳の内容や通話履歴の記録へアクセスするための「連絡先データを読み取り」の許可を求めるなどといったものがあります。Android端末にアプリをインストールする際に、不自然なアクセス許可や疑問に思うアクセス許可を求められた場合には、そのアプリのインストールを中止しましょう。

インストールしようとしているアプリケーションが、スマートフォンの中のどの情報／機能へアクセスするかという一覧。
※画面デザインは機種や状況により異なります。

図1-5：「アクセス許可」の表示画面の例

【5】セキュリティソフトを導入する。

スマートフォンの中でもAndroid端末では、2011年初頭以降大手ウイルス対策ソフトベンダーが続々とセキュリティソフトを発売し、その選択肢が充実してきました。Android端末では【4】に注意すればウイルスに感染する可能性を低減できますが、ゼロにはできません。ウイルス感染の可能性をより低減するためにセキュリティソフトを導入してください。

【6】スマートフォンを小さなパソコンと考え、パソコンと同様に管理する。

企業でスマートフォンを活用する場合、スマートフォンの利用ルール、スマートフォンからアクセス可能な情報の範囲、スマートフォンに保存してよい情報の範囲、紛失・盗難時の対応等のポリシーを定めましょう。特に端末管理（MDM：Mobile Device Management）によって、スマートフォンに搭載されているOSのアップデートの徹底やインストールできるアプリの制限等を企業側が強制的に管理できる仕組みを設けることをおすすめします。

今月のトピックス

- コンピュータ不正アクセス被害の主な事例（届出状況及び被害事例の詳細は、「3.コンピュータ不正アクセス届出状況」を参照）
  - サーバーの設定不備を突かれて侵入され、ファイルを置かれた
  - ファイアウォールに見知らぬルールが追加されていた
- 相談の主な事例 （相談受付状況及び相談事例の詳細は、「4.相談受付状況」を参照）
  - iPadでアダルトサイトにアクセスしたら、当該サイトの画面が消えなくなった
  - IPAと間違えて別の組織にワンクリック請求の対処を依頼してしまった
- インターネット定点観測（詳細は、別紙3を参照）
  IPA で行っているインターネット定点観測について、詳細な解説を行っています。

2. コンピュータウイルス届出状況 －詳細は別紙1を参照－

(1) ウイルス届出状況

7月のウイルスの検出数※1は、約**2.3**万個と、6月の約3.8万個から39.4%の減少となりました。また、7月の届出件数※2は、**1,064**件となり、6月の1,209件から12.0%の減少となりました。

※1 検出数 ： 届出にあたり届出者から寄せられたウイルスの発見数（個数）
※2 届出件数： 同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1日何個検出されても届出1件としてカウントしたもの。
・7月は、寄せられたウイルス検出数約2.3万個を集約した結果、1,064件の届出件数となっています。

検出数の1位は、**W32/Netsky**で約**1.0**万個、2位は**W32/Mydoom**で約**9.5**千個、3位は**W32/Autorun**で約**1.5**千個でした。

図2-1：ウイルス検出数

図2-2：ウイルス届出件数

(2) 不正プログラムの検知状況
7月は、特に目立った動きはありませんでした（図2-3参照）。

図2-3：不正プログラムの検知件数推移

3.　コンピュータ不正アクセス届出状況（相談を含む）　ー詳細は別紙2を参照ー

表**3-1** 不正アクセスの届出および相談の受付状況

	2月	3月	4月	5月	6月	7月
届出(a) 計	**10**	**6**	**5**	**7**	**9**	**8**
被害あり(b)	5	6	5	6	9	5
被害なし(c)	5	0	0	1	0	3
相談(d) 計	**23**	**45**	**38**	**55**	**32**	**47**
被害あり(e)	6	10	10	14	7	15
被害なし(f)	17	35	28	41	25	32
合計(a+d)	**33**	**51**	**43**	**62**	**41**	**55**
被害あり(b+e)	11	16	15	20	16	20
被害なし(c+f)	22	35	28	42	25	35

（**1**）不正アクセス届出状況
7月の届出件数は**8**件であり、そのうち何らかの被害のあったものは5件でした。

（**2**）不正アクセス等の相談受付状況
不正アクセスに関連した相談件数は47件であり、そのうち何らかの被害のあった件数は15件でした。

（**3**）被害状況
被害届出の内訳は、侵入**4**件、なりすまし**1**件でした。
「侵入」の被害は、データベースから設定情報が盗まれたものが1件、外部サイトを攻撃するツールを埋め込まれ、踏み台として悪用されていたものが2件、ファイルを勝手にアップロードされていたものが1件でした。侵入の原因は、設定不備が3件（アクセス制限の設定不備が2件、普段使用していない機能が有効になっていてその機能を使われたものが1件）で、他は原因不明でした。
「なりすまし」の被害は、本人になりすまして何者かにログインされ、IP電話サービスを勝手に利用されていたものが1件、でした。

（**4**）被害事例

[侵入]

(i) サーバーの設定不備を突かれて侵入され、ファイルを置かれた

事例	・組織外から「ウェブサーバーに対するアップロードの通信を検知した」との連絡が入った。 ・調査したところ、当該サーバーのウェブアプリケーション格納ディレクトリに、見知らぬファイルを発見。 ・当該サーバーではTomcatを使用しており、Tomcatのウェブアプリケーションマネージャ機能が有効になっていた。その機能を使用してファイルをサーバー上にアップロードされていた。 ・事後対策として、Tomcatのウェブアプリケーションマネージャ機能は不要であると判断したため、削除した。
解説・対策	使われていない機能が設定不備のまま放置されていたことが原因でした。 Tomcatのウェブアプリケーションマネージャは、ネットワーク経由でウェブアプリケーションを配備できるので便利な一方、悪用されると不正なファイルのアップロードに使用されてしまいます。同機能が不要の場合は機能の削除を、必要の場合は専用アカウントを作成した上で（パスワードは強固なものを使用して）運用することを勧めます。 一般的に、使われていない機能やサービスは管理や監視の対象から外れることになるため、セキュリティ対策漏れにつながります。当初は必要だった機能でも、現在は不要になっている可能性があります。サーバーで動作させる機能やサービスの棚卸しを、定期的に実施することをお勧めします。 （ご参考） ▶ IPA-安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/websecurity.html

[不正プログラム埋め込み]

(ii) ファイアウォールに見知らぬルールが追加されていた

事例	・社内規程に反するファイアウォールの設定を発見した。社内のあるサーバーに対して全ての通信を許可するルールになっていた。 ・当該サーバーを調査した結果、当該サーバーに不正なプログラムを埋め込まれて外部へのSSHスキャンの踏み台にされていた。 ・事後対策として、ファイアウォールの管理用パスワードを変更するとともに、ファイアウォール変更申請手続の実施を徹底するために実施方法の見直しを行った。 ・現在調査中だが内部犯行の可能性がある。
解説・対策	いくら社内文書で規定していても、技術的に可能な限り、社員による不正アクセスの脅威は常に存在します。対策の一環として、ファイアウォールを含めたネットワーク機器、および各種サーバーの管理用パスワードは強固なものにしてください。また共用のアカウントではなく、担当者ごとに個別のアカウントを発行し、有事の際に追跡可能にしておくことも重要です。 各種アクセスログの取得も必須ですが、そのことを社内にアナウンスすることで、社内犯行の抑止力になる場合があります。 （ご参考） ▶ IPA-情報セキュリティガバナンス http://www.ipa.go.jp/security/manager/know/meaning/governance.html

4. 相談受付状況

7月のウイルス・不正アクセス関連相談総件数は**1,490件**でした。そのうち『ワンクリック請求』に関する相談が**461件**（6月：511件）、『偽セキュリティソフト』に関する相談が**8件**（6月：11件）、**Winny** に関連する相

談が**7件**（6月：7件）、「情報詐取を目的として特定の組織に送られる不審なメール」に関する相談が**2件**（6月：6件）、などでした。

表4-1 IPA で受け付けた全ての相談件数の推移

		2月	3月	4月	5月	6月	7月
合計		1,521	1,723	1,608	1,640	1,692	1,490
	自動応答システム	892	1,106	997	950	999	889
	電話	570	551	555	620	639	540
	電子メール	53	58	50	62	50	54
	その他	6	8	6	8	4	7

（備考）
IPA では、「情報セキュリティ安心相談窓口」を開設し、コンピュータウイルス・不正アクセス、Winny 関連、その他情報セキュリティ全般についての相談を受け付けています。

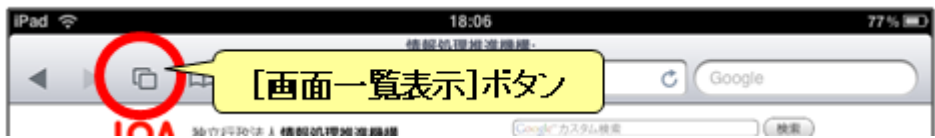
メール　**anshin@ipa.go.jp**
（これらのメールアドレスに特定電子メールを送信しないでください）
電話番号　03-5978-7509　（24時間自動応答、ただし IPA セキュリティセンター員による相談受付は休日を除く月～金、10:00～12:00、13:30～17:00のみ）
FAX　03-5978-7518　（24時間受付）
「自動応答システム」　：　電話の自動音声による応対件数
「電話」　：　IPA セキュリティセンター員による応対件数
合計件数には、「不正アクセスの届出および相談の受付状況」における『相談(d) 計』件数を内数として含みます。

図4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

(i)iPadでアダルトサイトにアクセスしたら、当該サイトの画面が消えなくなった

相談	iPadでアダルトサイトにアクセスしたら、当該サイトのページが張り付いた状態で消えなくなり、iPadを再起動しても残ったままになっている。 これはパソコンでいうところのワンクリック請求の症状が、iPadで起きているということか。iPadの場合はどうやって画面を消せばいいのか。
	この場合、**iPad**のブラウザである**Safari**のキャッシュや履歴として当該ページの情報が残っているために、**Safari**を開くたびにその情報を読み込んでしまい、画面が張り付いているように見えているということでしょう。**Safari**で［画面一覧

回答	表示］ボタンを押し、閉じたい画面の左上にある（X）を押すことで、再び画面が出てくる状況を解消することができます。 図4-2：iPadのSafariの画面上部 iPad上で請求画面を出すワンクリック請求の事例は、IPAではまだ確認していませんが、今後iPadでも同様の現象が起こりうる可能性は否定できませんので、ウェブサイトへのアクセスには十分注意してください。 （ご参考） ▶ IPA-「【注意喚起】ワンクリック請求に関する相談急増！ パソコン利用者にとっての対策は、まずは手口を知ることから！」 http://www.ipa.go.jp/security/topics/alert20080909.html

(ii) IPAと間違えて別の組織にワンクリック請求の対処を依頼してしまった

相談	パソコン上にアダルトサイトの請求画面が張りついて消えなくなった。 消費生活センターに相談したところ、請求画面を削除する方法については、IPAのウェブサイトを参照するように案内されたので、検索サイトで“IPA”を検索して、検索結果の上位に表示された組織のURLをIPAと思い込んでアクセスした。有料のサービスだったが電話対応してくれそうだったので、指示に従い請求画面を削除することができた。しかし、改めて当該組織のウェブサイトを確認してみたところ、IPAではなかったことに気付いた。 IPAで検索したはずなのに、一体どういうことなのか。
回答	あなたが対処を依頼した組織は、**IPA**とは無関係の別の組織です。 検索サイトでキーワード検索を行う際、必ずしも目的の情報が上位に表示されるとは限りません。また、検索サイトによっては、検索結果より上位に広告スポンサーの情報が表示される場合があります。 検索サイトで目的の情報を探す場合、検索結果に表示されるタイトル、**URL**、説明書きなどを十分確認し、間違った情報にアクセスしないようにしてください。 なお、IPAが公開しているワンクリック請求に関する情報については、以下のページを参照ください。 （ご参考） ▶ IPA-「【注意喚起】ワンクリック請求に関する相談急増！ パソコン利用者にとっての対策は、まずは手口を知ることから！」 http://www.ipa.go.jp/security/topics/alert20080909.html

5. インターネット定点観測での7月のアクセス状況

インターネット定点観測（TALOT2）によると、2011年7月の期待しない（一方的な）アクセスの総数は10観測点で**102,888**件、延べ発信元数※は**46,222**箇所ありました。平均すると、**1**観測点につき1日あたり**154**の発信元から**343**件のアクセスがあったことになります（図5-1参照）。

※延べ発信元数：TALOT2の各観測点にアクセスしてきた発信元を単純に足した数のことを、便宜上、延べ発信元数とする。ただし、同一発信元から同一の観測日・観測点・ポートに複数アクセスがあった場合は、発信元数を1としてカウントする。

TALOT2 における各観測点の環境は、インターネットを利用される一般的な接続環境と同一なので、インターネットを利用される皆さんの環境へも同じくらいの一方的なアクセスがあると考えられます。

※7月2日は保守作業のため、システムを停止しています。そのため、7月の観測データは、この1日を除外して統計情報を作成しています。なお、通常は常時稼動しています。

図5-1：1観測点・1日あたりの期待しない(一方的な)平均アクセス数と発信元数

2011年2月～2011年7月までの各月の1観測点・1日あたりの平均アクセス数とそれらのアクセスの平均発信元数を図5-1に示します。7月の期待しない（一方的な）アクセスは、6月と比べて大きく減少しました。
6月と7月の宛先（ポート種類）別アクセス数の比較を図5-2に示します。445/tcpが大きく減少したにもかかわらず、増加が観測されたのは11083/tcpからのアクセスでした。

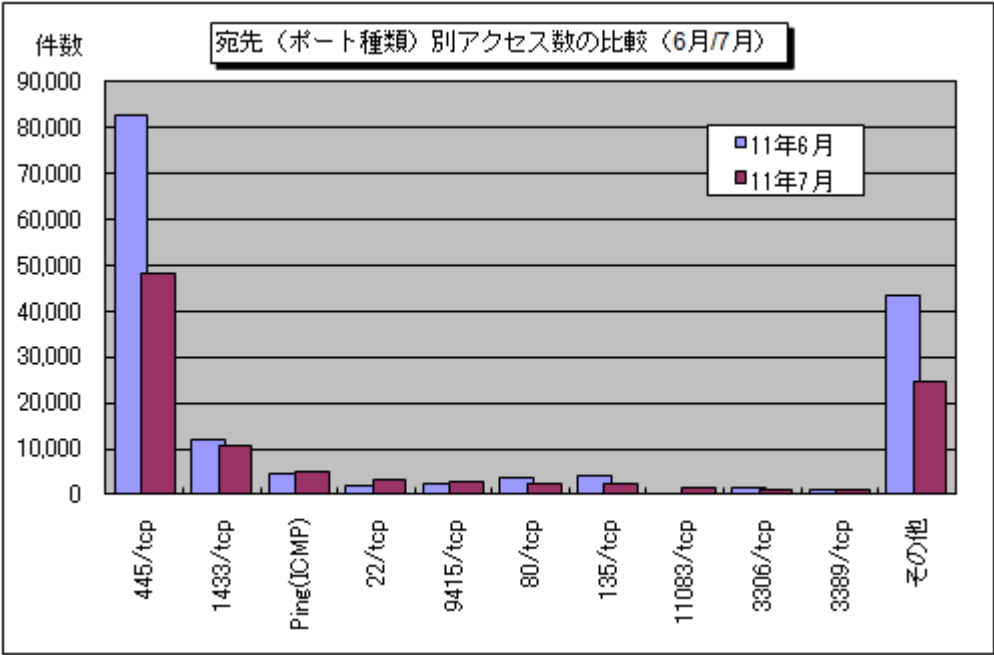



図5-2：宛先（ポート種類）別アクセス数の比較（6月/7月）

11083/tcpは、7月3日以降にTALOT2の特定の１観測点で観測され始めたアクセスであり、発信元地域はアメリカと中国が大部分を占めていました（図5-3参照）。このポートは特定のアプリケーションで使用されるポートというわけではなく、このアクセスが何を目的としたものだったかは不明です。

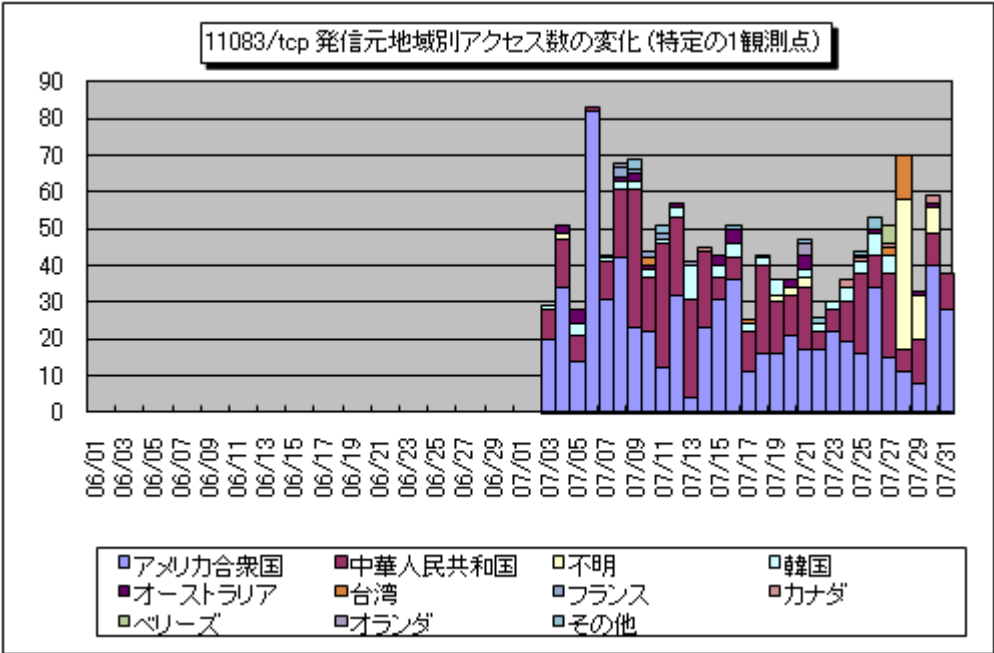



図5-3：11083/tcp発信元地域別アクセス数の変化（特定の1観測点）

以上の情報に関して、詳細はこちらのPDFファイルをご参照ください。

- 別紙3_インターネット定点観測（TALOT2）での観測状況について

届出の詳細については以下の PDF ファイルをご参照ください。

- 本紙_コンピュータウイルス・不正アクセスの届出状況[7月分]
- 別紙1_コンピュータウイルスの届出状況について［詳細］
- 別紙2_コンピュータ不正アクセスの届出状況について［詳細］

『他機関・ベンダーの各種統計情報は以下のサイトで公開されています。』

一般社団法人JPCERTコーディネーションセンター：http://www.jpcert.or.jp/
@police：http://www.cyberpolice.go.jp/
フィッシング対策協議会：http://www.antiphishing.jp/
株式会社シマンテック：http://www.symantec.com/ja/jp/
トレンドマイクロ株式会社：http://jp.trendmicro.com/jp/home/
マカフィー株式会社：http://www.mcafee.com/japan/

お問い合わせ先：

独立行政法人 情報処理推進機構 技術本部 セキュリティセンター（IPA/ISEC）
（ISEC：Information technology SEcurity Center）
TEL：03-5978-7591 FAX：03-5978-7518
E-mail： isec-info@ipa.go.jp
（このメールアドレスに特定電子メールを送信しないでください）
URL：http://www.ipa.go.jp/security/

ページトップへ

情報セキュリティ

ENGLISH

- 読者層別
  - 個人の方
  - 経営者の方
  - システム管理者の方
  - 技術者・研究者の方
- 緊急対策情報
- 届出・相談
  - ウイルスの届出
  - 不正アクセスの届出
  - 脆弱性関連情報の届出
- 情報セキュリティ対策
  - ウイルス対策
  - ボット対策
  - 不正アクセス対策
  - 脆弱性対策
  - 対策実践情報
- 暗号技術
- セキュリティエコノミクス
- 情報セキュリティ認証関連
  - JISEC
  - JCMVP
- セミナー・イベント
- 資料・報告書・出版物
- ツール
- 公募
- サポート情報
  - 用語集
  - FAQ（よくある質問）
  - セキュリティ関連リンク
- セキュリティセンターについて

コンピュータウイルス・不正アクセスの届出状況[4月分]について

第12-09-245号
掲載日：2012年 5月 7日
独立行政法人情報処理推進機構
技術本部 セキュリティセンター

IPA (独立行政法人情報処理推進機構、理事長：藤江 一正)は、2012年4月のコンピュータウイルス・不正アクセスの届出状況をまとめました。
(届出状況の詳細PDF資料はこちら)

1. 今月の呼びかけ

「 あなたを狙うスマホアプリに要注意！ 」
～不正なアプリをインストールしてしまわないために～

2012年4月、スマートフォン（Android OS）のアプリケーションの公式マーケットで、不審な動きをする不正なアプリが多数発見されました。公式マーケットに表示されるダウンロード総数から、おおよそ7万回以上のダウンロードが行われたと考えられます。
その不正なアプリは「ほかのスマートフォンOSで人気のアプリ」「有名なアプリ名、アイコンが使われている」「興味を持たせるキーワードが含まれている」といった、スマートフォン利用者に対して強い興味を抱かせる「だましのテクニック」が使われています。

不正なアプリをインストールし実行することで、スマートフォンの端末情報や、アドレス帳の中身が外部に送信されることが確認されています。個人情報やプライバシー情報が流出してしまうため、こうした情報が悪質な行為に利用される可能性があります。
ここでは、このような手口を明らかにし、被害にあわないための対策を解説します。

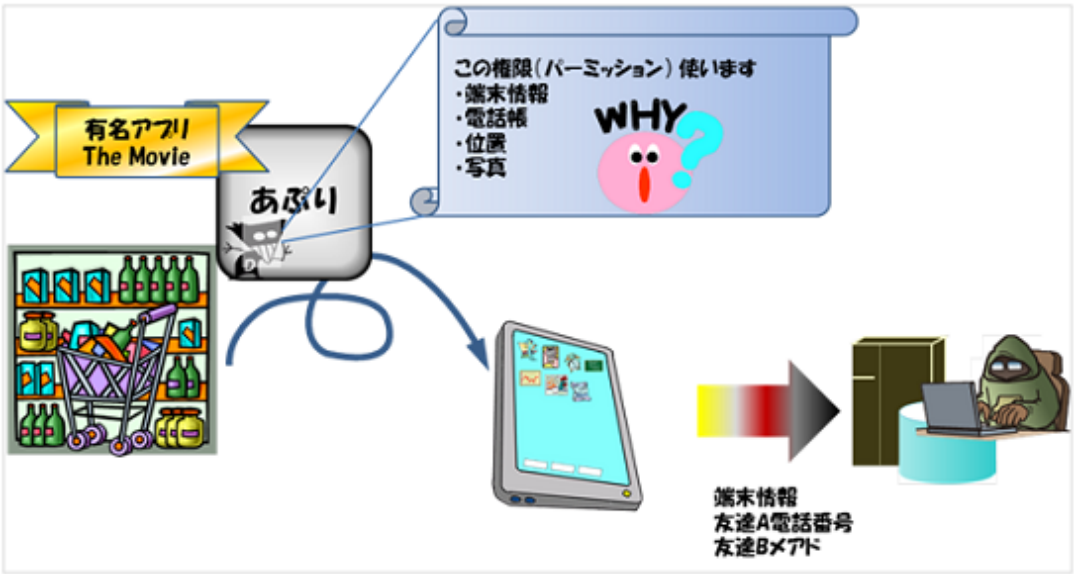



図1-1：不正なアプリが情報を流出させるイメージ図

(1)特徴
Android OS用アプリの公式マーケットである“Google Play”に、次のような特徴を持つ「動画を表示することを連想させるようなアプリ」が発見されました。これらのアプリ

は、動画の再生前に勝手に端末の情報やアドレス帳の情報を外部のサーバに送信するようになっていました。また、インストールするとマーケットで説明されている名称と異なった名前で表示されるということも特徴的です。

表1-1：発見された不正なアプリの例

項番	特徴	アプリ配布場所における名称	インストール後の名称
1	有名なアプリ、ほかのスマートフォンOSで人気のアプリ名を含む	ウォーリーを探せ the Movie	ユーチューブ動画
		うまい棒をつくろう！ the Movie	youtube動画まとめ
		ギャングハウンド the Movie	グラビア動画
		スヌーピーストリート the Movie	笑える動画
		チャリ走-the Movie	ようつべ動画まとめ
		ぴよ盛り the Movie	面白動画まとめ
		メガ盛ポテト the Movie	芸能動画
		空手チョップ! The Movie	ニコニコ動画まとめ
		大盛モモ太郎 the Movie	youtube動画
		桃太郎電鉄the Movie	ようつべ動画
		魔界村騎士列伝 THE MOVIE	暇つぶし動画
		連打の達人 the Movie	ユーチューブ動画まとめ
2	個人的嗜好をくすぐる文字列を含む	ＦＣ２動画まとめ the Movie	怖い動画
		けいおん-K-ON!動画	アニメ動画
		スク水動画まとめ	美人動画
3	実用性を感じさせる文字列を含む	3D視力回復 THE MOVIE	泣ける動画

上記アプリ以外にも、複数のセキュリティ関連組織において同種の動きをするアプリが確認されており、おおよそ30種類以上のアプリがAndroid OS用の公式マーケットであるGoogle Playに存在していたことが明らかになっています。なお、その対象アプリ自体は現在Google Playから削除されていますが、以前Google Playに表示されていたダウンロード数からおおよそ7万回以上インストールされている可能性が指摘されています。

今回、IPAでは不正なアプリの一つを使って検証を実施しました。ここでは、インストールをするときに表示される権限許可の問い合わせ画面や、アンインストール方法を紹介します。さらに、このような不正なアプリを見分けるためのテクニックも紹介します。

紹介にあたっては、Android OSを使用している「GALAXY Tab SC-01C（Android OS 2.2）」を利用し、その画面を元に説明します。OSのバージョンや機種によっては、画面や操作方法が異なる場合があります。なお、現在はAndroid OS用の公式マーケットから同アプリは削除されていますが、別の場所からインストールすることは危険ですので試してはいけません。

今回紹介する不正なアプリをインストールする際、Google Playからダウンロードを行う前に、アプリが必要とする権限の確認画面が表示されます。権限確認画面で「同意してダウンロード」または「インストール」を行うと、表示された権限の選択に従ってこのアプリが端末内の情報にアクセスしたり、動作したりすることを許可してしまいます。Google Play以外からインストールを行う場合、背景色や文字の色が異なることにも注目してください。

図1-2：Google Playの場合（例）

図1-3：Google Play以外の場合（例）

図1-4：アプリに対して権限を許可するイメージ図

なお、今回の不正アプリが必要とする権限は次のとおりでした。

表1-2 今回発見された不正なアプリが必要とする権限

	権限（パーミッション）名	許可した場合にどうなるか（抜粋）
1	電話発信	アプリが端末に付与されている電話番号や、端末識別番号、SIM情報などを読み取ることができます。 電話の着信状態などの情報も読み取ることができます。
2	個人情報	アプリがアドレス帳など連絡先データを読み取ることができます。
3	ネットワーク通信	アプリがインターネットなどにある外部のサーバーと自由に通信できます。

IPAでこのアプリを解析したところ、このアプリはandroid_id（端末の識別子）と端末の電話番号を特定のサーバーへ送信するようになっていました。この送信が成功すると、次にアドレス帳に登録された名前、電話番号、Eメールアドレスを全て送信します。これらの送信が成功後、特定のサーバーから動画を取得、再生する仕組みとなっていました。

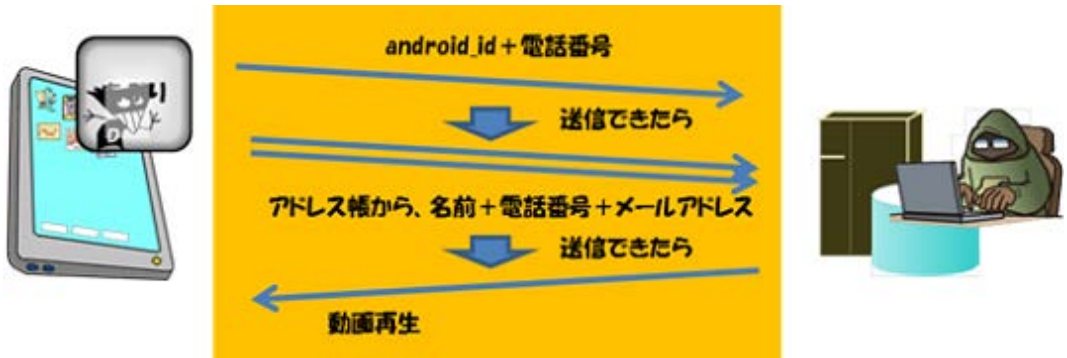



図1-5：テストした不正なアプリの簡易解析結果

もし、このようなアプリをインストールしてしまった場合、アプリがどのような権限を持っているかを調べ、アンインストールすることができます。

図1-6：インストール済みアプリの権限（パーミッション）の確認方法とアンインストール方法

(2) 類似事例

今回発見された不正なアプリは、端末の情報とアドレス帳の情報を勝手に外部のサーバーに送信する動作をするものでしたが、IPAではこれまでにも次のような不正なアプリを確認しています。いずれのアプリも、インストール時に必要以上の権限を取得しようとしています。（図1-7、1-8、1-9参照）

表1-3：その他の不正なアプリ例

	不正なアプリの種類	主な特徴
1	ワンクリック請求アプリ※1	電話番号などの端末情報を外部に送信する。
2	ボット型ウイルス※2	外部からの操作指令を受けてアドレス帳データやSMSの送信をしたり、地図やWebページを表示したりする。
3	不正発信アプリ	勝手に電話を発信する。（特定の国でのみ動作し、日本では動かない。）

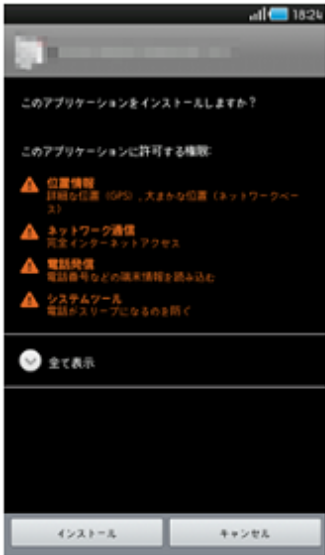



図1-7：ワンクリック請求アプリ例

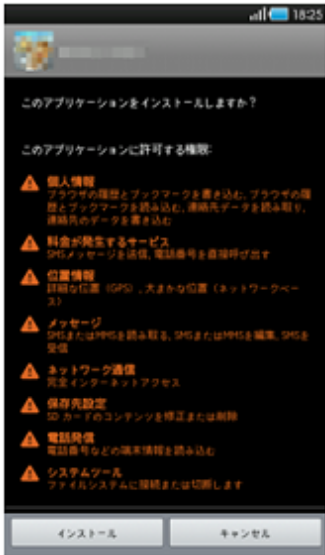



図1-8：ボット型ウイルス例

図1-9：不正発信アプリ例

（※1）「スマートフォンでもワンクリック請求に注意！」
http://www.ipa.go.jp/security/txt/2012/02outline.html
（※2）Android OSを標的としたウイルスに関する注意喚起
http://www.ipa.go.jp/security/topics/alert20110121.html

(3)対策

IPAでは、これまでもスマートフォンを安全に使うための対策を発表※3、※4してきましたが、特に今回は利用者の増えているAndroid OSを使ったスマートフォンについて、“スマートフォンを安全に使うための六箇条”から抜粋して、具体的な対策を紹介していきます。

表1-4 スマートフォンを安全に使うための六箇条

①	スマートフォンをアップデートする。
②	スマートフォンにおける改造行為を行わない。
③	信頼できる場所からアプリケーション（アプリ）をインストールする。
④	アンドロイド端末では、アプリをインストールする前に、アクセス許可を確認する。
⑤	セキュリティソフトを導入する。
⑥	スマートフォンを小さなパソコンと考え、パソコンと同様に管理する。

（※3）スマートフォンを安全に使おう！～スマートフォンを安全に使用するための６箇条～
http://www.ipa.go.jp/security/txt/2011/08outline.html
（※4）スマートフォンのセキュリティ<危険回避>対策のしおり
http://www.ipa.go.jp/security/antivirus/documents/08_smartphone.pdf

その**1**）信頼できる場所からアプリを入手しよう（六箇条 ③）
Android OSを使用したスマートフォンは、アプリを入手する方法が複数ありますが、中には不正なアプリも存在します。信頼のおけるアプリを選んで紹介するページなどを利用することで、不正なアプリをインストールしてしまう危険性が低減できます。なお、Androidの設定画面に「提供元不明のアプリ」という項目があります。この項目のチェックを外しておくことで、Google Playからのみアプリをインストールできるようになります。
操作を誤るなどして不正なアプリをインストールしてしまわないよう、普段はこの項目のチェックを外した状態にしておくことを勧めます。
なお、信頼できる第三者のマーケットであっても、Google Play以外で入手したアプリケーションをインストールする際は、一時的にこの設定を変更する（チェックを入れる）必要があります。その場合、インストール終了後、再度チェックを外してください。

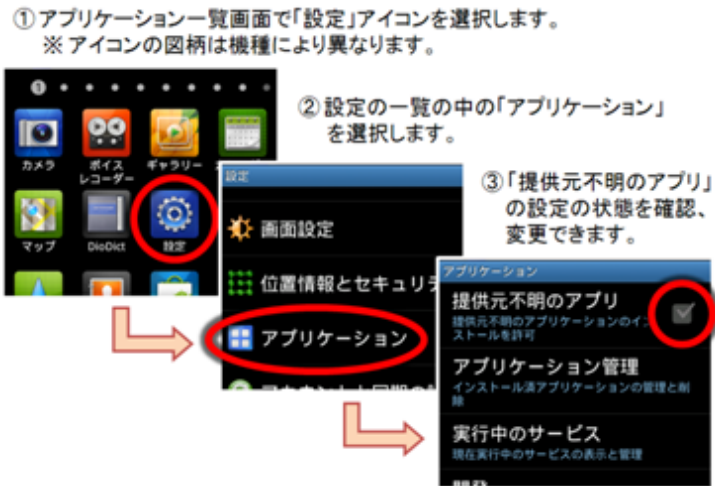



図1-10：「提供元不明のアプリ」のインストール許可設定画面

その**2** ）アプリをインストールする際に必要とされる権限（パーミッション）を確認しよう
（六箇条 ④）
アプリをインストールするときに表示される権限（パーミッション）をよく確認してください。例えば、動画再生や画像表示アプリなのに、電話を発信する権限を求めてくる、カメラ機能が必要なさそうなアプリなのに、写真を撮る権限を求めてくるような場合は、怪しいアプリと言えます。

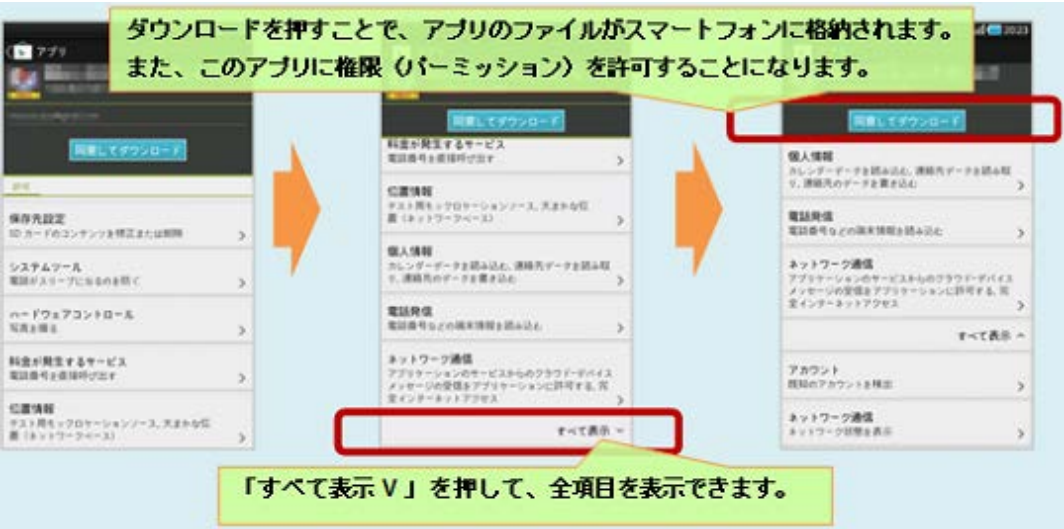



図1-11：権限（パーミッション）の確認画面

なお、上記例の権限（パーミッション）を正当に必要とするアプリもあります。一見必要なさそうな権限の許可を求めていても、確実に不正なアプリであると判断することは難しいのが実情です。次項のセキュリティソフト（アプリ）での検知や、（4）一歩踏み込んだおすすめの対策での情報収集を行うことで、総合的に判断をしてください。

その**3** ）セキュリティソフト（アプリ）を利用しよう（六箇条 ⑤）
アプリはインストールしただけでは動いていないことがほとんどです。通常は「インストール終了」をきっかけにセキュリティソフト（アプリ）によるスキャンが始まることが多いので、セキュリティソフト（アプリ）による診断結果をよく確認してください。場合によっては、ウイルス検知された当該アプリを自分でアンインストールすることが必要となります。

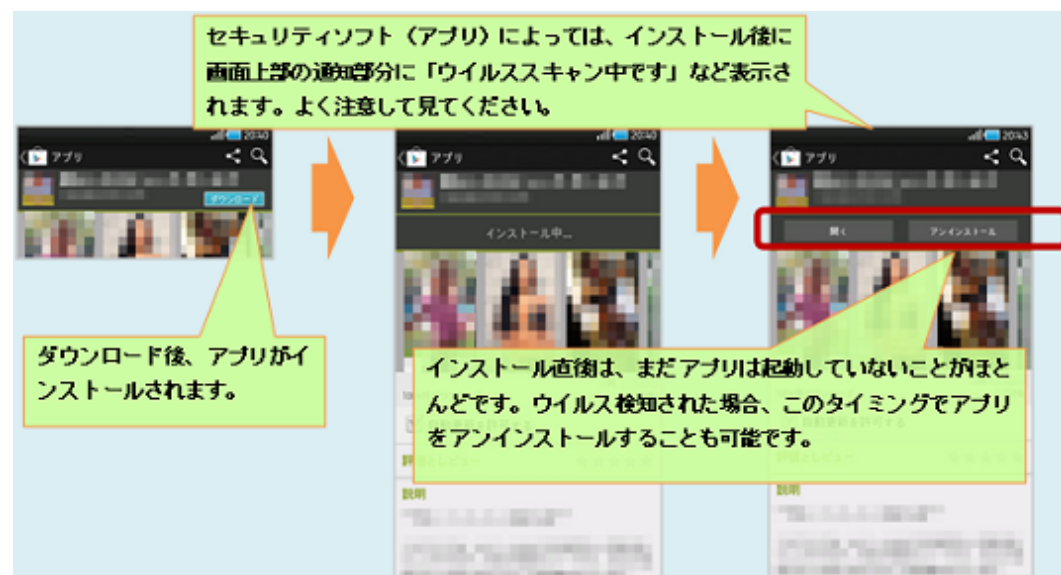



図1-12：アプリのダウンロードからインストールまでの流れ

その4）アプリを最新の状態に保とう（六箇条 ①・⑥）
アプリの更新があった場合は最新の状態にしてください。アプリの自動更新を設定することで、自動的に最新の状態にすることも可能です。
近年、スマートフォンの利用者数は増加傾向にあり、利用者数に比例するようにスマートフォンに関する脆弱性も多数報告されています※5。脆弱性を解消したアプリをいち早く利用するようにしてください。

（※5 ）脆弱性対策情報データベースJVN iPediaの登録状況[2012年第1四半期（1月～3月）]
http://www.ipa.go.jp/security/vuln/report/JVNiPedia2012q1.html

図1-13：アプリの自動更新許可方法

アプリの更新有無は、Google Playで確認できます。また、アプリ更新前と必要とする権限が異なる場合、確認画面が表示されますのでよく内容を確認してください。

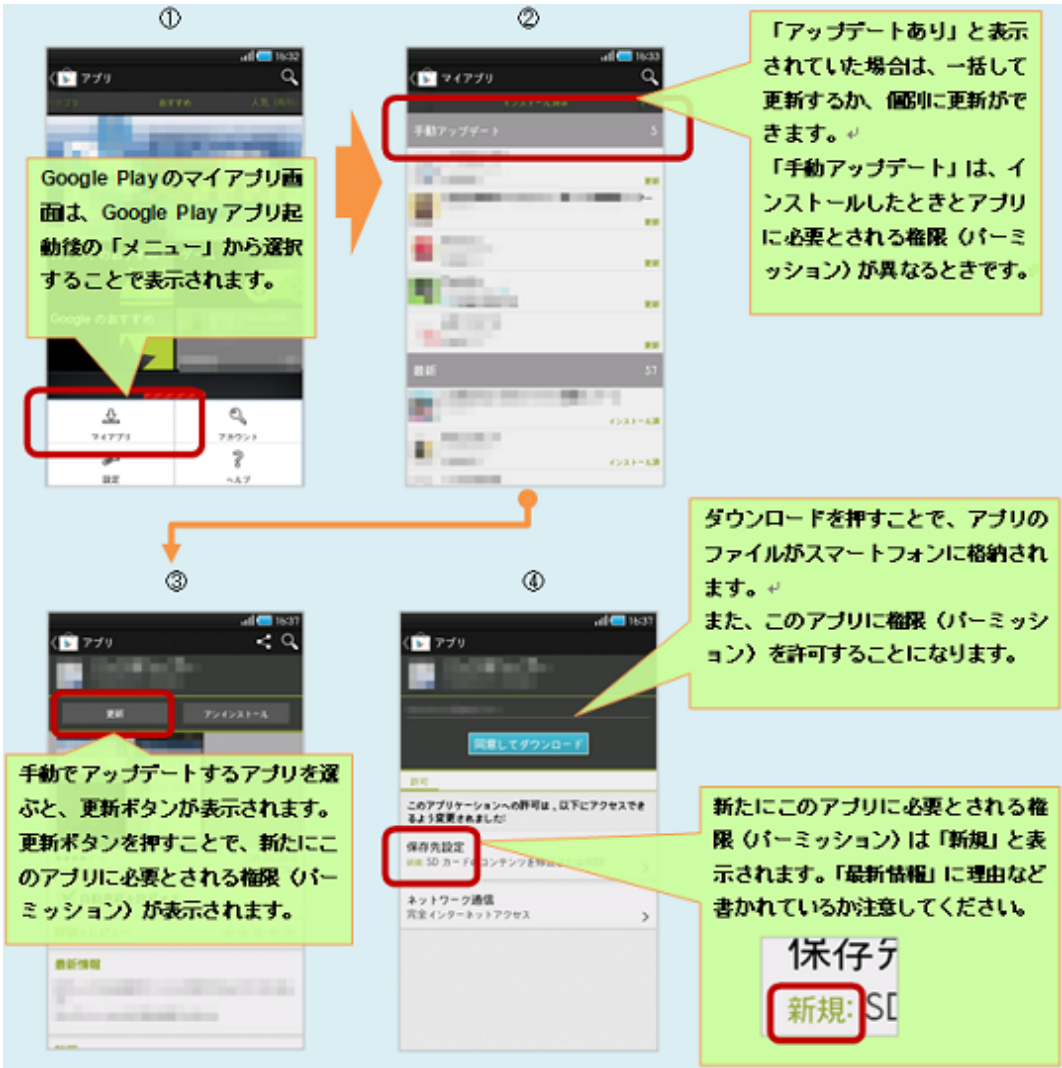



図1-14：アプリの更新例

(4)一歩踏み込んだおすすめの対策

アプリは安心な配布場所から入手するようにして、ダウンロードの前にアプリが必要とする権限を確認し、インストール後にセキュリティアプリのスキャン結果を確認することを紹介しましたが、これ以外にも、一歩踏み込んだおすすめの対策として、「アプリをインストールする際の情報収集のコツ」を紹介します。

アプリを選ぶとき、画面にはたくさんの重要な情報が記載されています。その情報をできる限り読み取ってください。悪い評判や噂がある場合、ひとまず、インストールを控えることをお勧めします。

〜インストール前に行う情報収集の例〜
○レビュー記事に悪い評判は書かれていないか
○アプリ開発者が他に公開しているアプリの評判に、悪いものがないか
○開発者やアプリ名をインターネットで検索して、悪い評判や噂などはないか

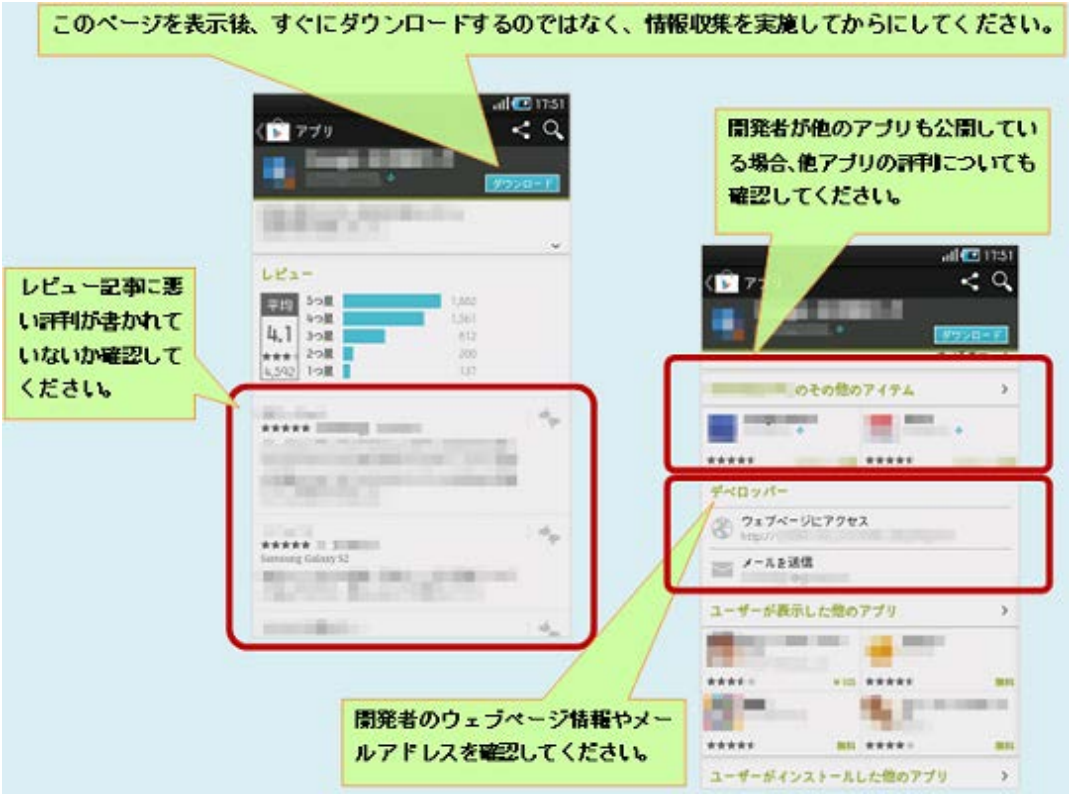



図1-15：アプリに関する情報収集の例

今月のトピックス

- コンピュータ不正アクセス被害の主な事例（届出状況及び被害事例の詳細は、「3.コンピュータ不正アクセス届出状況」を参照）
  - 古いメールアカウントを不正使用され、大量のスパムメールを送信された
  - ブルートフォース攻撃によって侵入され、ウェブサイトを改ざんされた
- 相談の主な事例 （相談受付状況及び相談事例の詳細は、「4.相談受付状況」を参照）
  - Internet Explorer のブラウザ画面が次から次へと出てきて止まらなくなった
  - 自分が管理しているブログを見ると、偽セキュリティ対策ソフト型ウイルスに感染する？

2. コンピュータウイルス届出状況 －詳細は別紙1を参照－

(1) ウイルス届出状況

4月のウイルスの検出数※1は、**10,339**個と、3月の15,841個から34.7%の減少となりました。また、4月の届出件数※2は、**732**件となり、3月の866件から15.5%の減少となりました。

※1 検出数 ： 届出にあたり届出者から寄せられたウイルスの発見数（個数）
※2 届出件数： 同じ届出者から寄せられた届出の内、同一発見日で同一種類のウイルスの検出が複数ある場合は、1日何個検出されても届出1件としてカウントしたもの。
・4月は、寄せられたウイルス検出数10,339個を集約した結果、732件の届出件数となっています。

検出数の1位は、**W32/Mydoom**で**5,150**個、2位は**W32/Netsky**で**3,646**個、3位は**W32/Downad**で**622**個でした。

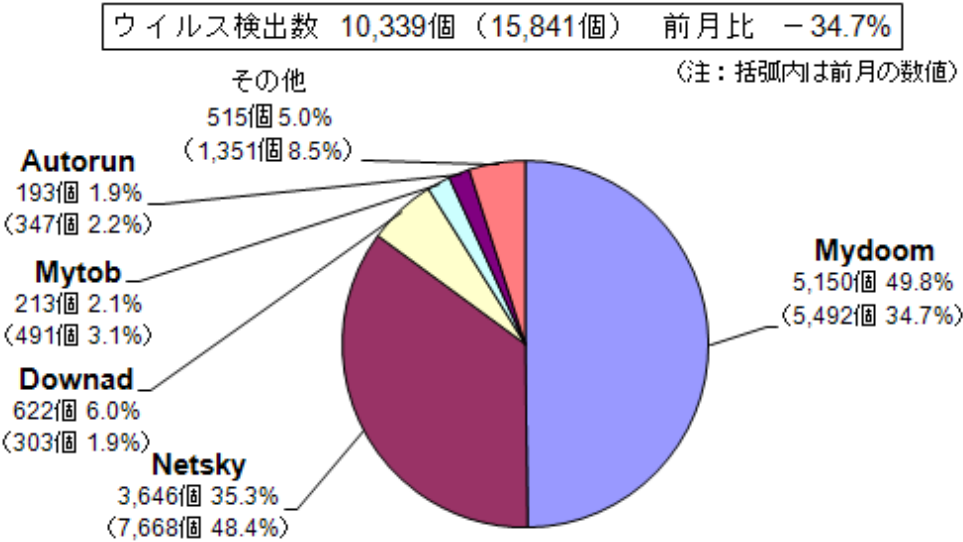



図2-1：ウイルス検出数

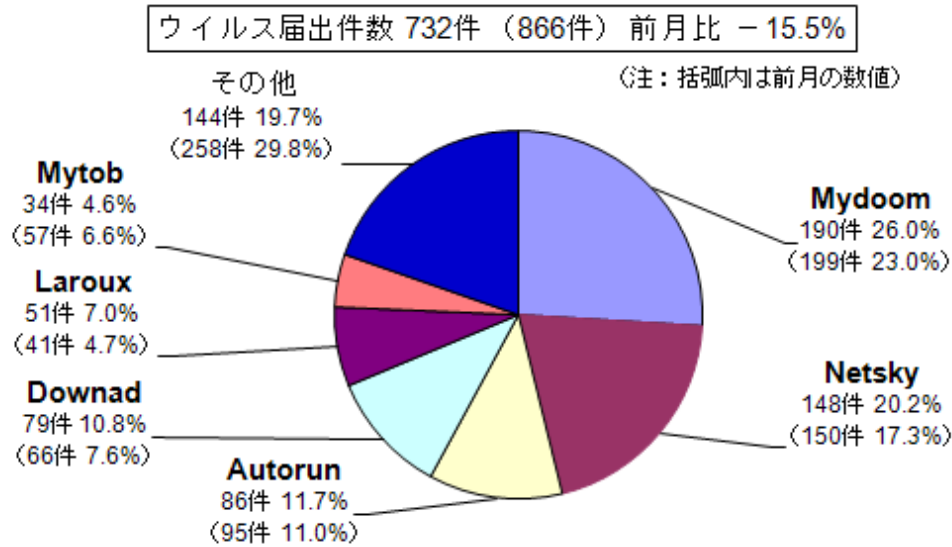



図2-2：ウイルス届出件数

(2) 不正プログラムの検知状況

4月は、別のウイルスを感染させせようとするDOWNLOADER、オンラインバンキングのID／パスワードを詐取するBANCOSといった不正プログラムが増加傾向となりました。（図2-3参照）。

※ ここでいう「不正プログラムの検知状況」とは、IPAに届出られたものの中から「コンピュータウイルス対策基準」におけるウイルスの定義に当てはまらない不正なプログラムについて集計したものです。
※ コンピュータウイルス対策基準：平成12年12月28日（通商産業省告示 第952号）（最終改定）（平成13年1月6日より、通商産業省は経済産業省に移行しました。）
「コンピュータウイルス対策基準」（経済産業省）
http://www.meti.go.jp/policy/netsecurity/CvirusCMG.htm

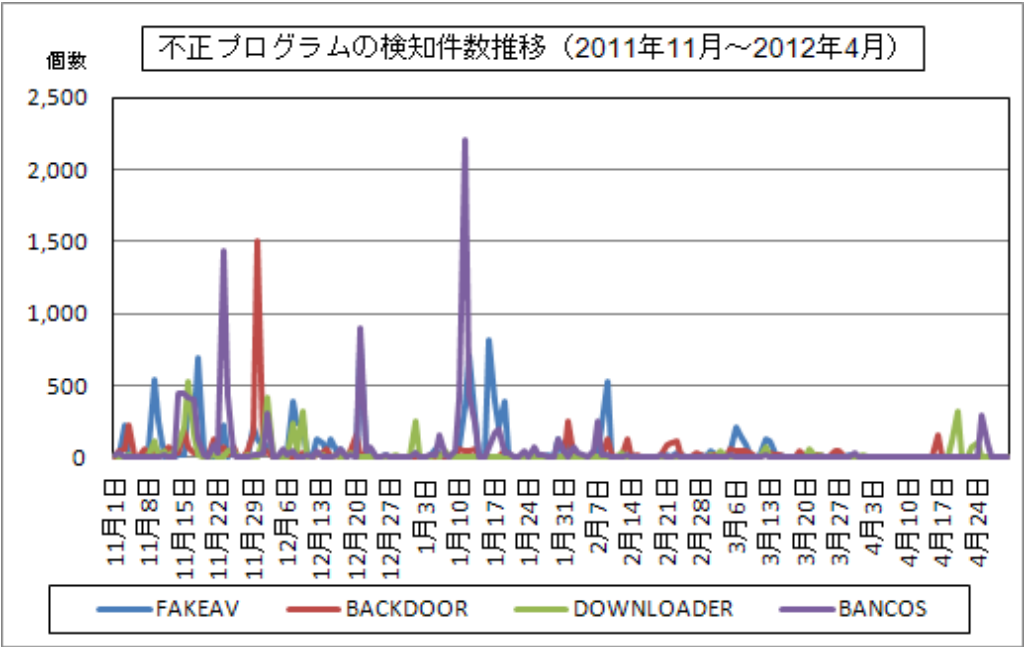



図2-3：不正プログラムの検知件数推移

3. コンピュータ不正アクセス届出状況（相談を含む） ー詳細は別紙2を参照ー

表3-1 不正アクセスの届出および相談の受付状況

		11月	12月	1月	2月	3月	4月
届出(a) 計		7	7	8	13	5	9
	被害あり(b)	5	7	7	9	4	7
	被害なし(c)	2	0	1	4	1	2
相談(d) 計		69	42	35	37	54	46
	被害あり(e)	14	13	9	14	10	9
	被害なし(f)	55	29	26	23	44	37
合計(a+d)		76	49	43	50	59	55
	被害あり(b+e)	19	20	16	23	14	16
	被害なし(c+f)	57	29	27	27	45	39

（1）不正アクセス届出状況

4月の届出件数は9件であり、そのうち何らかの被害のあったものは7件でした。

（2）不正アクセス等の相談受付状況

不正アクセスに関連した相談件数は46件であり、そのうち何らかの被害のあった件数は9件でした。

（3）被害状況

被害届出の内訳は、侵入4件、なりすまし3件でした。
「侵入」の被害は、ウェブページが改ざんされていたものが4件（内、ウイルスをダウンロードさせるように改ざんされていたものが2件）でした。侵入の原因は、CMSの脆弱性を悪用されたものが1件、ネットワーク経由のブルートフォース攻撃により管理者権限を奪われたものが1件、サーバーの設定不備が1件でした（他は原因不明）。
「なりすまし」の被害は、オンラインサービスに本人になりすまして何者かにログインされ、サービスを勝手に利用されていたものが2件、メールアカウント悪用されてスパムメールを送信されたものが1件、でした。

（4）被害事例

[なりすまし]

(i)古いメールアカウントを不正使用され、大量のスパムメールを送信された

事例	・社内のあるメールアカウントから、大量のスパムメールが送信されていることに気付いた。 ・当該メールアカウントの持ち主は既に退社していた。また単純なパスワードを設定していたので、アカウントハックによるなりすましの可能性が高い。 ・当該アカウントを削除するとともに、安易なパスワードを設定しないよう改めて社内に周知した。
解説・対策	退職者のメールアカウントを廃棄せず放置しているうちに、第三者に乗っ取られて悪用されてしまった例です。 古いアカウントが残っていると、退職者にそのまま使われ続けたり、今回のケースのように第三者に乗っ取られたりする恐れがあります。メールアカウントに限らず、ユーザーアカウントの棚卸しを定期的に実施することをお勧めします。特に異動や退職が多数発生する年度の変わり目の時期には、可能な限り棚卸しを実施してください。

[侵入]

(ii）ブルートフォース攻撃によって侵入され、ウェブサイトを改ざんされた

事例	・商用サイトを運営しているが、ある日、ウェブサイト閲覧者から「ページを見ただけでウイルスをダウンロードさせられた」との連絡が入った。 ・すぐに状況を確認すると、確かにウェブサイトは改ざんされており、ページを閲覧するだけで「Security Shield」という偽セキュリティ対策ソフトをダウンロードさせるように改ざんされていた。 ・原因調査の結果、サーバーに対する、ネットワーク経由でのブルートフォース（力ずく）攻撃により管理者権限アカウントのパスワードを破られて、サーバーに侵入されたことが分かった。 ・対策として、パスワードを20文字以上にするとともに、改ざん検知システムを導入した。
解説・対策	ウェブサイト改ざん被害に留まらず、ウイルス配布サイトとして悪用されてしまった例です。 ブルートフォース攻撃への対策は、パスワードを強固なものにすることが基本ですが、アカウントロック機能（ログインの試行回数を超えたアカウントへのアクセスを一時停止させる機能）を使用することも有効です。この機能を使用することで、攻撃者のログイン試行回数が減少し、結果として侵入される可能性が小さくなります。 サーバーOSの機能で、パスワードの複雑性や有効期間を強制できる場合は、その機能を使用することも検討してください。

4. 相談受付状況

4月のウイルス・不正アクセス関連相談総件数は**750件**でした。そのうち『ワンクリック請求』に関する相談が**131件**（3月：130件）、『偽セキュリティソフト』に関する相談が**26件**（3月：44件）、**Winny** に関連する相談が**7件**(3月：6件）、「情報詐取を目的として特定の組織に送られる不審なメール」に関する相談が**3件**（3月：3件）、などでした。

表4-1 IPA で受け付けた全ての相談件数の推移

		11月	12月	1月	2月	3月	4月
合計		1,420	1,312	1,302	1,073	772	750
	自動応答システム	746	790	760	645	427	428
	電話	561	451	485	362	287	270
	電子メール	102	65	49	62	49	50
	その他	11	6	8	4	9	2

（備考）
IPA では、「情報セキュリティ安心相談窓口」を開設し、コンピュータウイルス・

不正アクセス、Winny 関連、その他情報セキュリティ全般についての相談を受け付けています。

メール　**anshin@ipa.go.jp**
（これらのメールアドレスに特定電子メールを送信しないでください）
電話番号　03-5978-7509 （24時間自動応答、ただし IPA セキュリティセンター員による相談受付は休日を除く月～金、10:00～12:00、13:30～17:00のみ）
FAX　03-5978-7518 （24時間受付）

「自動応答システム」 ： 電話の自動音声による応対件数
「電話」 ： IPA セキュリティセンター員による応対件数
合計件数には、「不正アクセスの届出および相談の受付状況」における『相談(d)計』件数を内数として含みます。

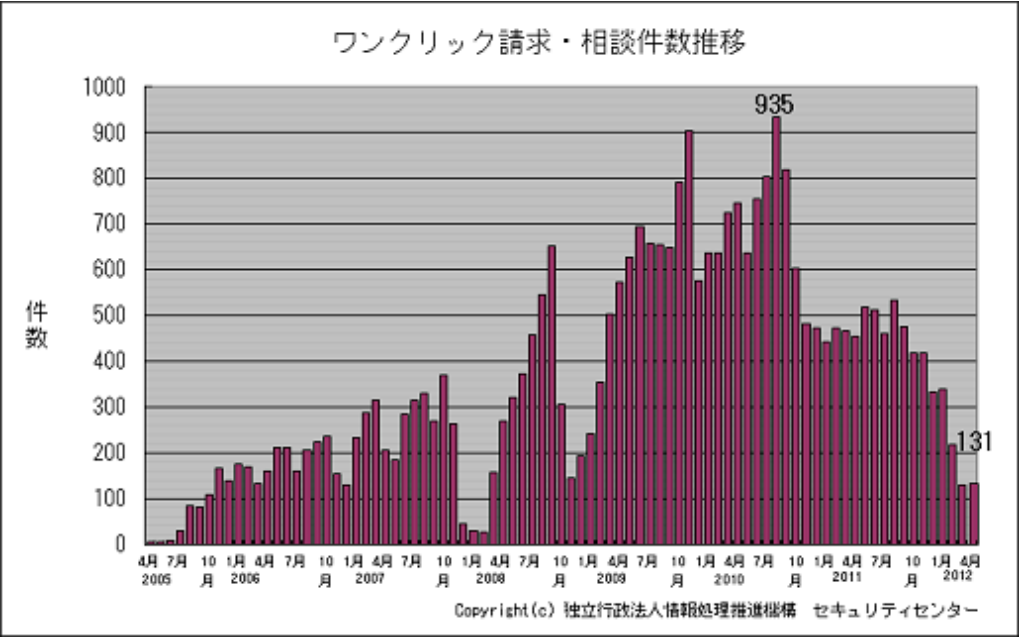



図4-1：ワンクリック請求相談件数の推移

主な相談事例は以下の通りです。

(i) Internet Explorer のブラウザ画面が次から次へと出てきて止まらなくなった

相談	インターネットに接続し、いろいろなサイトを見ていたのだが、変なサイト（アダルトサイトだと思う）を表示してしまったようでブラウザ画面が次々と表示されて、止まらなくなってしまった。その後、セキュリティソフトでは何も検出されなかった。パソコン再起動後、今は正常に使えている。 何が起きたのか？
回答	Internet Explorerのブラウザ画面が次々と出てきて、止まらなくなる現象という事ですが、これは「ブラウザクラッシャー」による症状と思われます。対処方法としてはブラウザのキャッシュをクリアし、再起動後、同様な症状が出ないか少し様子を見て下さい。今後の対策としては、不用意に変なサイトへアクセスしないことが最も大切です。また**URL**フィルタリング機能や有害サイトブロック機能付きの統合型セキュリティソフトを利用することが有効策となります。

(ii) 自分が管理しているブログを見ると、偽セキュリティ対策ソフト型ウイルスに感染
する？

相	自分が所属している団体のブログ（WordPressを使用）がウイルスに感染しているのではないかと思っている。そのブログを見るとSystem Checkという偽セキュリティ対策ソフトに感染してしまうという報告が何件も届いている。ブ

談	ログを正常に戻す方法を教えてもらえないか。ブログは、今も停止していない。
回答	現在レンタルサーバを利用し、簡単にブログを開設しているとの事ですが、そのブログで使われているシステムの脆弱性を突くことで**System Check**という偽セキュリティ対策ソフト型ウイルスを感染させる仕掛けが仕込まれている可能性が高いです。まず、サイト内のページに身に覚えのない**HTML**タグやスクリプト文が追加されていないか確認してください。また、ブログシステムのバージョンを確認し、必要に応じて**WordPress**や利用中のテーマ、プラグインのアップデートを必ず実施して下さい。 （ご参考） ▶ IPA- 安全なウェブサイトの作り方 http://www.ipa.go.jp/security/vuln/documents/website_security.pdf

届出の詳細については以下の PDF ファイルをご参照ください。

- 本紙_コンピュータウイルス・不正アクセスの届出状況[4月分]
- 別紙1_コンピュータウイルスの届出状況について［詳細］
- 別紙2_コンピュータ不正アクセスの届出状況について［詳細］

『他機関・ベンダーの各種統計情報は以下のサイトで公開されています。』

一般社団法人JPCERTコーディネーションセンター：http://www.jpcert.or.jp/
@police：http://www.cyberpolice.go.jp/
フィッシング対策協議会：http://www.antiphishing.jp/
株式会社シマンテック：http://www.symantec.com/ja/jp/
トレンドマイクロ株式会社：http://jp.trendmicro.com/jp/home/
マカフィー株式会社：http://www.mcafee.com/japan/
株式会社カスペルスキー：http://www.viruslistjp.com/analysis/

お問い合わせ先：

独立行政法人 情報処理推進機構 技術本部 セキュリティセンター
TEL：03-5978-7591 FAX：03-5978-7518
E-mail： isec-info@ipa.go.jp
（このメールアドレスに特定電子メールを送信しないでください）
URL：http://www.ipa.go.jp/security/

更新履歴：

▶ 2012年 5月 7日 掲載

ページトップへ

Android OSを標的とした不審なアプリに関する注意喚起

第12-11-247号

掲載日：2012年 5月23日
独立行政法人情報処理推進機構
技術本部 セキュリティセンター（IPA/ISEC）

Android OSを標的とした不審なアプリに関する注意喚起

2012年4月、スマートフォン（Android OS）のアプリケーションの公式マーケットで、不審な動きをする不正なアプリが多数発見されました。この不正アプリをインストールし実行することで、スマートフォンの端末情報や、アドレス帳の中身が外部に送信されることが確認されており、警察による捜査が進んでいます。
このたび、公式マーケットではない場所で、同様の動きをする不審なアプリが確認されました。
5月中旬には当機構の情報セキュリティ安心相談窓口に、このアプリによる被害相談も寄せられています。本注意喚起では、今回見つかった不審なアプリの概要を解説するとともに、対策を示します。
解説にあたっては、Android OSを使用している「GALAXY Tab SC-01C（Android OS 2.2）」を利用し、その画面を元に説明します。OSのバージョンや機種によっては、表示される文字や画面、操作方法が異なる場合があります。なお、現在同アプリは削除されていますが、別の方法などでインストールすることは危険ですので試してはいけません。

1.不審なアプリの入手経路

このアプリは、公式マーケットではなく一般のウェブサイトからダウンロードできるものでした。
アプリ自体は、複数のブログや、アプリ紹介サイトで紹介されていて、アプリ名に興味を持ったスマートフォン利用者にダウンロードさせるような、だましのテクニックが使われています。
中には、公式マーケット（Google Play）からのインストールを装い、ボタンをタッチすると確認もないままアプリのファイルをダウンロードするサイトも発見されました。
スマートフォンの設定で「提供元不明のアプリ」を許可してしまうと、ダウンロード完了後にインストール開始画面となり、さらにインストール時にアプリが必要とする権限を許可してしまうと、アプリがインストール完了してしまいます。
インストール後の画面に表示される「開く」ボタンか、アプリのアイコンをタッチすると、このアプリが起動してしまいます。

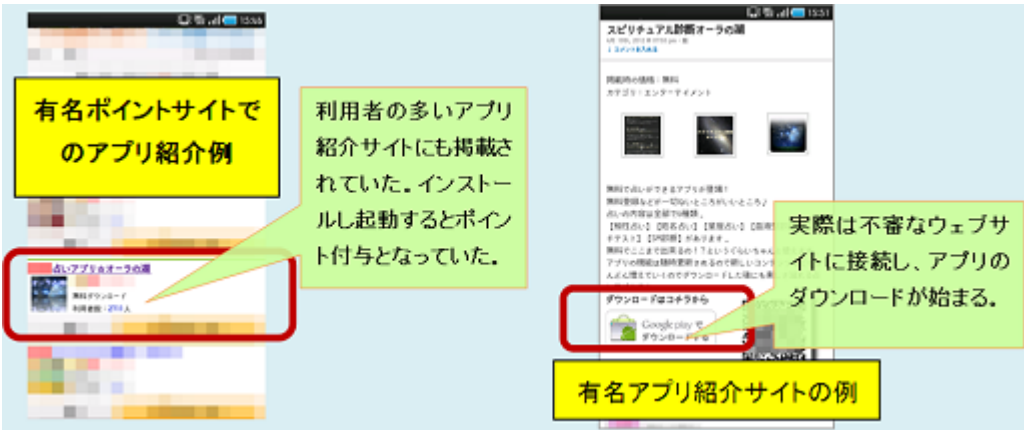



図1：紹介サイトの例

2.不審なアプリの特徴

2.1.インストール時の特徴

不審なアプリは次のようなアプリ名でブログやアプリ紹介サイトに掲載されていることを確認しています。これ以外の媒体（メールやSNS）についても、同様の特徴を備えたものが紹介されている可能性があります。

アプリ名：「占いアプリオーラの湖」

このアプリは次のようなステップでインストールされます。
「紹介サイトでアプリボタンをタッチ」→「アプリダウンロード」→「インストール画面」→「インストール完了」
アプリは、インストール後に利用者が自発的にアプリを起動しない限り、起動しませんでした。
また、公式マーケット以外で配布されているため、インストール画面でアプリが必要とする権限（パーミッション）確認画面は、黒色背景となります。まず、この画面配色で一度注意を払うことが望ましいです。

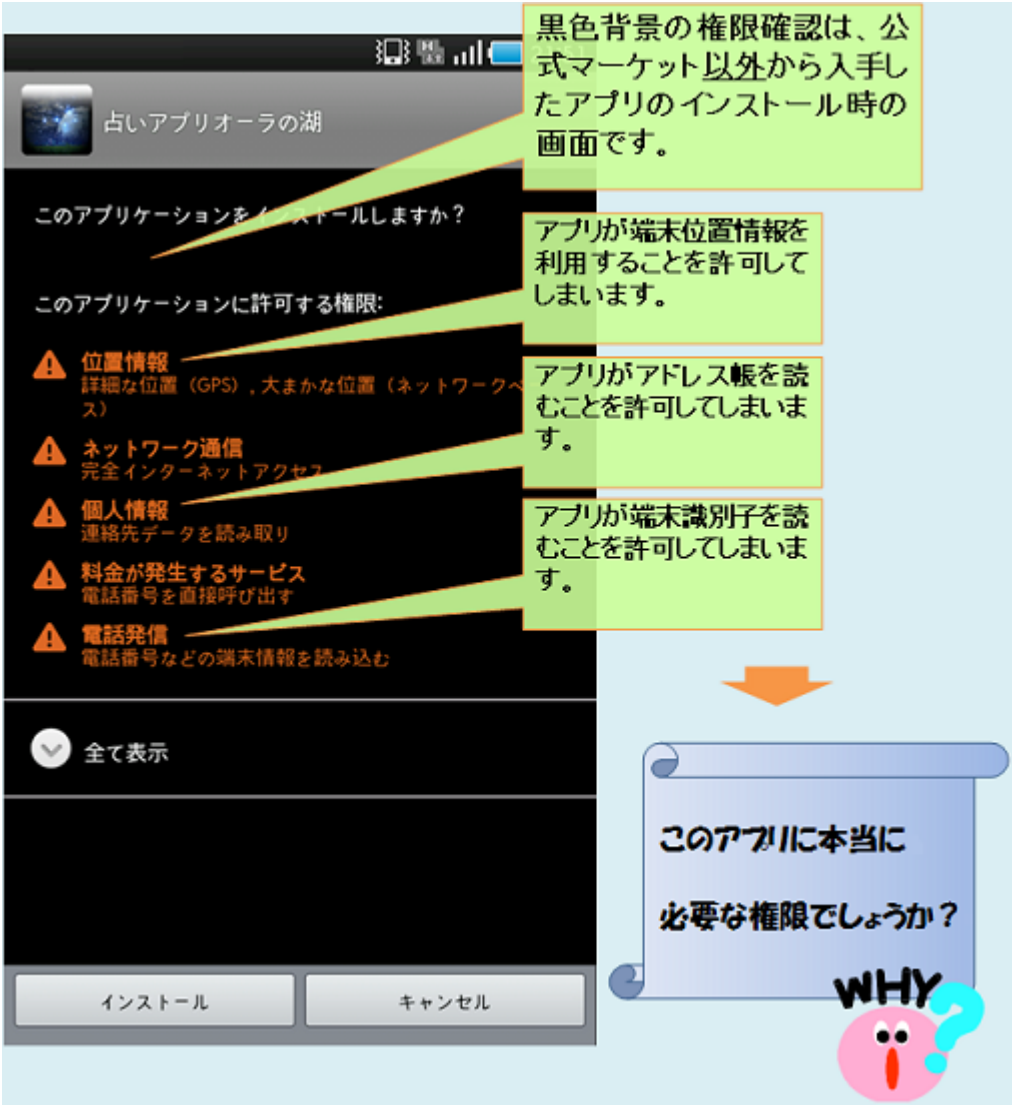



図2：不審なアプリの特徴（インストール時）

2.2.起動時の特徴

このアプリは、起動後に端末の情報やアドレス帳の内容などを収集します。アプリは一見それらのデータをランダムに抽出・表示し、その日に連絡しあう人を推奨しますが、その裏でログファイルを作成し、あらかじめ設定された不審なサイト宛に、端末の情報を送信します。

アプリ中央のボタンをタッチすると、「ちょっとお待ち下さい。」「占い中・・・」と表示し、アドレス帳のデータを収集開始します。アドレス帳のデータを収集後、別の不審なサイトに端末や回線の識別情報とアドレス帳に登録された名前、電話番号、メールアドレスを送付します。

なお、アドレス帳に登録が全くない場合は「アドレス帳に何も登録されてないよ～」と表示し、登録がある場合はランダムに抽出したアドレスの一つを表示します。

ちなみに、アプリの表示上部のバナーをタッチすると、出会い系サイトのページが表示されるようになっていました。

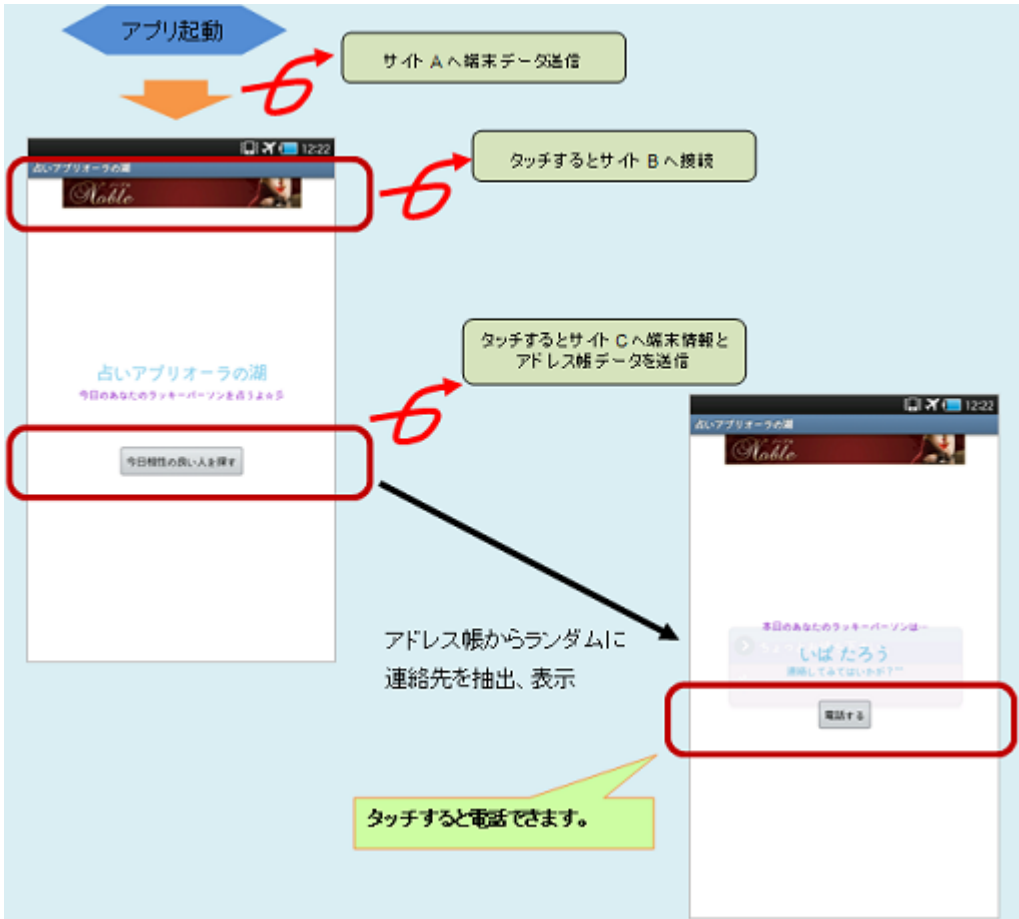



図3：不審なアプリの特徴（実行時）

3.今後の対策

今後も同様の不審なアプリが出現する可能性があります。特に注意すべきなのは、以下の2点です。

- アプリのインストール時に表示される、アプリが必要とする権限の内容に注意する。（図2参照）
- アプリは信頼できる場所から入手する。特に、公式マーケット以外から入手したアプリには細心の注意を払う。なお、公式マーケット以外から入手したアプリは、アプリインストール時の画面の背景が黒地になるため、容易に判別が可能。（図2参照）

IPAでは、これまでもスマートフォンを安全に使うための対策方法を発表※1、※2、※3してきました。そちらに記載した内容も参照し、より安心してスマートフォンを利用できるようにしてください。

（※1）あなたを狙うスマホアプリに要注意！ ～不正なアプリをインストールしてしまわない
ために～
http://www.ipa.go.jp/security/txt/2012/05outline.html

（※2）スマートフォンを安全に使おう！～スマートフォンを安全に使用するための６箇条～
http://www.ipa.go.jp/security/txt/2011/08outline.html

（※3）スマートフォンのセキュリティ<危険回避>対策のしおり
http://www.ipa.go.jp/security/antivirus/documents/08_smartphone.pdf

4.ご参考

この不審なアプリについて、5月21日にIPAから警視庁サイバー犯罪対策課に情報を提

供しました。同日19時ごろには、当該アプリのダウンロードはできなくなっていました。

本件に関するお問い合わせ先

IPA 技術本部 セキュリティセンター （**IPA / ISEC**） 加賀谷／青木
TEL：03-5978-7591 FAX：03-5978-7518 E-mail： isec-info@ipa.go.jp
（このメールアドレスに特定電子メールを送信しないでください）

報道関係からのお問い合わせ先

IPA 戦略企画部 広報グループ 横山／大海
Tel: 03-5978-7503 Fax:03-5978-7510 E-mail: pr-inq@ipa.go.jp
（このメールアドレスに特定電子メールを送信しないでください）

更新履歴

- 2012年05月23日 掲載